Department of Homeland Security
Information Analysis and Infrastructure Protection Directorate
CyberNotes

Issue #2003-14 *July 14, 2003*

CyberNotes is published every two weeks by the Department of Homeland Security/Information Analysis and Infrastructure Protection (IAIP) Directorate. Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between June 24 and July 11, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Adobe Systems Incorporated [1]	Unix	Acrobat Reader (UNIX) 5.05-5.0 7, 4.05	A buffer overflow vulnerability exists in the 'WWWLaunchNetscape' function when hyperlinks are processed, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Adobe Unix Acrobat Reader Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proofs of Concept exploit scripts have been published.
AIDeX [2]	Multiple	Mini-Webserver 1.1	A vulnerability exists because some directories are inadequately protected, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Mini-Webserver Information Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[1] Sec-labs Team Advisory, June 29, 2003.
[2] SecurityFocus, July 7, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Alexander Konig[3]	Unix	terminator X 3.80	A buffer overflow vulnerability exists in the 'HOME' and 'XLOCALEDIR' environment variables due to insufficient validation of user-supplied input, which could let a malicious user execute arbitrary code with root privileges.	No workaround or patch available at time of publishing.	TerminatorX 'HOME' & 'XLOCALE DIR' Environment Variable Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
Anope IRC Services[4]	Multiple	Anope Services 1.4.15-1.4.20, 1.4.25	A Denial of Service vulnerability exists in 'operserv' when a malicious client submits a raw message requesting to join a channel.	No workaround or patch available at time of publishing.	Anope Services Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability can be exploited with an IRC client.
Apache Software Foundation[5]	Windows, MacOS X 10.x, Unix	Apache 2.0.43-2.0.46	A Denial of Service vulnerability exists due to an error in the type-map handler when parsing type maps.	Upgrade available at: http://httpd.apache.org/download.cgi	Apache Web Server Type-Map Denial of Service	Low	Bug discussed in newsgroups and websites.
Apache Software Foundation[6, 7]	Windows, MacOS X 10.x, Unix	Apache 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.46	A remote vulnerability exists when the 'SSLCipherSuite' directive is used to upgrade a cipher suite, which could cause a weaker cipher suite being used.	**Apache Software Foundation:** http://httpd.apache.org/download.cgi **Trustix:** ftp://ftp.trustix.net/pub/Trustix/updates/2.0/RPMS/	Apache Web Server SSLCipher Suite Weak Cipher Suite CVE Name: CAN-2003-0192	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Apache Software Foundation[8, 9]	Windows, MacOS X 10.x, Unix	Apache 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.46	A remote Denial of Service vulnerability exists in the FTP proxy component when a target server that has an IPV6 address format is specified.	**Apache Software Foundation:** http://httpd.apache.org/download.cgi **Trustix:** ftp://ftp.trustix.net/pub/Trustix/updates/2.0/RPMS/	Apache Web Server FTP Remote Denial of Service CVE Name: CAN-2003-0254	Low	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[3] Bugtraq, July 9, 2003.
[4] SecurityFocus, July 8, 2003.
[5] SNS Advisory No.66, July 9, 2003.
[6] Apache Security Announcement, July 9, 2003.
[7] Trustix Secure Linux Security Advisory, 2003-0025, July 11, 2003.
[8] Apache Security Announcement, July 9, 2003.
[9] Trustix Secure Linux Security Advisory, 2003-0025, July 11, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Foundation[10, 11]	Windows, MacOS X 10.x, Unix	Apache 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.46	A remote Denial of Service vulnerability exists in the prefork Multi-Processing Module (MPM).	**Apache Software Foundation:** http://httpd.apache.org/download.cgi **Trustix:** ftp://ftp.trustix.net/pub/Trustix/updates/2.0/RPMS/	Apache Web Server Prefork MPM Remote Denial of Service CVE Name: CAN-2003-0253	Low	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Apple[12]	MacOS X 10.2	MacOS X 10.2-10.2.6	A buffer overflow vulnerability exists in the screen saver password feature, which could let a malicious user cause obtain unauthorized access.	No workaround or patch available at time of publishing.	MacOS X Screen Saver Password Buffer Overflow	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Aprelium Technologies[13]	Unix	Abyss Web Server 1.1.2	Several vulnerabilities exist: a buffer overflow vulnerability exists in HTTP GET requests due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code; and an input validation vulnerability exists in the 'Location:' header returned in a '302 Found' page, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.aprelium.com/news/abws116b1.html	Abyss Web Server HTTP GET Heap Overrun	**High**	Bug discussed in newsgroups and websites. There is no exploit code required for the input validation vulnerability.
a-suivre.net[14]	Windows, Unix	iXmail 0.2, 0.3	Several vulnerabilities exist: a vulnerability exists in the 'ixmail_netattach.php' script due to insufficient sanitization of user-supplied input for certain URI parameters, which could let a malicious user delete arbitrary files; a vulnerability in the 'Index.PHP' script, which could let a remote malicious bypass the authentication procedure and obtain sensitive information; and a file upload vulnerability exits in the 'ixmail_attach.php' script due to insufficient sanitization of user-supplied URI parameters, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	iXmail Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published for the 'ixmail_netattach.php' vulnerability. There is no exploit code required for the 'ixmail_attach.php' vulnerability.

[10] Apache Security Announcement, July 9, 2003.
[11] Trustix Secure Linux Security Advisory, 2003-0025, July 11, 2003.
[12] Securiteam, July 6, 2003.
[13] Securiteam, July 1, 2003.
[14] SecurityTracker Alert ID, 1007054, June 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Axis Communications[15]	Multiple	Print Server 560 6.10, 6.15, 6.20, Print Server 5600 6.10, 6.15, 6.20	A Denial of Service vulnerability exists when a malicious HTTP request is submitted.	Upgrade available at: ftp://ftp.axis.com/pub_soft/prt_srv/	Axis Print Server Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Bahamut Team[16]	Unix	andromede.net Andromede IRCd 1.2.3-Release; DALnet Bahamut IRCd 1.4.35; digatech digatech IRCd 1.2.1; IRCd-RU! IRCd-RU! 1.0.6 – release, 1.0.6 -03-stable, 1.0.6 -02-stable, 1.0.6 -01-stable; methane methane IRCd 0.1.1	A format string vulnerability exists when Behamut is compiled with 'DEBUGMODE' defined, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	Upgrade available at: ftp://ftp.ircd.ru/pub/ircd-RU/ircd-RU-1.0.6-04-stable.tar.gz	Bahamut IRCd Remote Format String	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit script has been published.
BEA Systems, Inc.[17]	Windows NT 4.0/2000, Unix	WebLogic Express & Server 6.1, SP1-SP5, 7.0, SP1&SP2, 7.0 .0.1, SP1&SP2, 8.1, WebLogic Express/ Server for Win32 6.1, SP1-SP5, Win32 7.0, SP1&SP2, Win32 7.0.0.1, SP1&SP2	A vulnerability exists when a firewall, connection filter or other mechanism is used to restrict access to the console and MSI (managed server independence), which could let a remote malicious user bypass security restrictions and obtain unauthorized access.	Patches available at: ftp://ftpna.beasys.com/pub/releases/security/	WebLogic Server / Express Unauthorized Console Access	Medium	Bug discussed in newsgroups and websites.

[15] Securiteam, July 8, 2003.
[16] 0xbadc0ded Advisory #01, June 26, 2003.
[17] BEA Security Advisory, BEA03-32.00, July 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
BEA Systems, Inc.[18]	Windows NT 4.0/2000, Unix	WebLogic Express & Server 6.1, SP1-SP5, 7.0, SP1&SP2, 7.0 .0.1, SP1&SP2, 8.1, WebLogic Express/ Server for Win32 6.1, SP1-SP5, Win32 7.0, SP1&SP2, Win32 7.0.0.1, SP1&SP2	A vulnerability exists in Node Manager Keyfile because the password is passed on the commandline in plaintext, which could let a malicious user obtain sensitive information.	Patches available at: ftp://ftpna.beasys.com/pub/releases/security/	BEA WebLogic / Server Node Manager Password	Medium	Bug discussed in newsgroups and websites.
BEA Systems, Inc.[19]	Windows NT 4.0/2000, Unix	WebLogic Express / Server 6.1, SP1-SP5, 7.0, SP1&SP2, 7.0 .0.1, SP1&SP2, 8.1, WebLogic Express/ Server for Win32 6.1, SP1-SP5, Win32 7.0, SP1&SP2, Win32 7.0.0.1, SP1&SP2	A vulnerability exists when there are users in the Operator role who are not also in the Admin role and the NodeManager is used to start servers, which could let malicious user obtain sensitive information.	Patches available at: ftp://ftpna.beasys.com/pub/releases/security/	BEA WebLogic Server/Express Operator Role	Medium	Bug discussed in newsgroups and websites.
Bill Wilson[20]	Unix	GKrellM Mailwatch Plugin 2.4.1, 2.4.2	A buffer overflow vulnerability exists, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	GKrellM Mailwatch Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[18] BEA Security Advisory, BEA03-34.00, July 8, 2003.
[19] BEA Security Advisory, BEA03-33.00, July 8, 2003.
[20] SecurityFocus, July 7, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Billing Explorer[21]	Windows	Game.Net Series 4.43, Grand Series 4.43, Web-Base Edition 4.43	A vulnerability exists due to insufficient authentication or confidentiality between the client and the server, which could let a remote malicious user modify billing data, shutdown a client, and obtain the administrator's password.	No workaround or patch available at time of publishing.	BillingExplorer Insufficient Authentication	Low/ Medium/ **High** **(Low if the client is shut down; Medium if data is modified; and High if adminis-trative access can be obtained)**	Bug discussed in newsgroups and websites.
BiT SHiFT-ER[22]	Windows, Unix	BiT BOARD 2.0	A vulnerability exits because the password database is insufficiently secured, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Bitboard Password Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
BRS[23]	Windows NT	Web Weaver 1.04, 1.0 3	A Cross-Site Scripting vulnerability exists due to a lack of input validation, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.brswebweaver.com/modules.php?op=modload&name=News&file=article&sid=3	WebWeaver Error Page Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Canon[24]	Multiple	GP-300	A remote Denial of Service vulnerability exists when handling some types of malformed web requests.	No workaround or patch available at time of publishing.	Canon GP300 Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
CCBILL LLC [25]	Multiple	CCBill whereami.cgi	A vulnerability exists in the 'whereami.cgi' script because some types of input are not handled properly, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	CCBill WhereAmI.cgi Script	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[21] Xnuxer Research Security Report, July 8, 2003.
[22] Bugtraq, July 9, 2003.
[23] Secunia Research Advisory, June 26, 2003.
[24] Bugtraq, July 7, 2003.
[25] Secunia Security Advisory, July 7, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cerulean Studios[26]	Windows NT	Trillian 0.74, 1.0	A remote Denial of Service vulnerability exists when a corrupt 'TypingUser' message is submitted.	No workaround or patch available at time of publishing.	Trillian Client Malformed TypingUser Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability may be exploited using a modified Trillian client.
Changshin Soft Co., Ltd. [27]	Windows	ezTrans Server	A Directory Traversal vulnerability exists in the 'download.php' script, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	EZTrans Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Cisco Systems[28]	Multiple	Catalyst 4000 Series including models 2948G & 2980G/2980G-A, 5000 Series including models 2901, 2902 & 2926, Catalyst 6000	A remote Denial of Service vulnerability exists when handling a non-standard combination of TCP flags.	Patches available at: http://www.cisco.com/warp/public/707/cisco-sa-20030709-swtcp.shtml	Cisco Catalyst Non-Standard TCP Flags Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability can be exploited with one of several free, publicly available network testing utilities. Vulnerability has appeared in the press and other public media.
cPanel[29]	Unix	cPanel 5.0, 5.3, 6.0, 6.2, 6.4-6.4.2, 6.4.2 .STABLE_48	A vulnerability exists in the 'Error Log' and 'Latest Visitors' screens due to insufficient sanitization of HTTP requests, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrade available at: http://www.cpanel.net/downloads.htm	CPanel Admin Interface HTML Injection	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
CREN[30] ***Exploit script published*** [31]	**Unix**	**ListProc 8.2.9**	**A buffer overflow vulnerability exists in the 'ULISTPROC_UMASK' environment variable due to insufficient bounds checking, which could let a malicious user execute arbitrary code.**	**No workaround or patch available at time of publishing.**	**ListProc ULISTPROC_UMASK Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.** ***Exploit script has been published.***

[26] Bugtraq, July 4, 2003.
[27] STG Security Advisory, SSA-20030701-03, July 8, 2003
[28] Cisco Security Advisory Rev. 1, 43864, July 10, 2003.
[29] Securiteam, July 8, 2003.
[30] Secure Network Operations, Inc. Advisory, SRT2003-05-08-1137, May 8, 2003.
[31] SecurityFocus, July 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
CutePHP Team[32]	Unix	CuteNews 1.3	A Cross-Site Scripting vulnerability exists in posted messages due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	CuteNews Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
ddskk/skk [33]	Unix	ddskk 11.6.rel.0; skk 10.62 a	A vulnerability exists when temporary files are created due to insufficient security precautions, which could let a malicious user obtain elevated privileges.	Upgrades available at: http://security.debian.org/pool/updates/main/d/ddskk/ http://security.debian.org/pool/updates/main/s/skk/	SKK/DDSKK Insecure Temporary Files	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Debian[34]	Unix	Linux 3.0	A vulnerability exists because temporary files are created insecurely, which could let a malicious user overwrite arbitrary files.	Upgrade available at: http://security.debian.org/pool/updates/main/s/semi/	SEMI/WEMI Insecure Temporary File Creation CVE Name: CAN-2003-0440	Medium	Bug discussed in newsgroups and websites.
Debian[35]	Unix	Linux 3.0	A vulnerability exists because temporary files are created insecurely, which could let a malicious user overwrite arbitrary files.	Upgrade available at: http://security.debian.org/pool/updates/main/x/x-face-el/x-face-el_1.3.6.19-1woody1_all.deb	X-Face-EL Insecure Temporary File Creation	Medium	Bug discussed in newsgroups and websites.
Deerfield [36]	Windows NT	VisNetic Website 3.5.13 .1, 3.5.15, 3.5.17	A path disclosure vulnerability exists when a request is made for a nonexistent CGI resource, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.deerfield.com/download/visnetic_website/	VisNetic Website Nonexistent CGI Resource	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Early Impact[37]	Windows	Product Cart 2br000, 2, 1.6br003, 1.6br001, 1.6br, 1.6b003, 1.6b002, 1.6b001, 1.6b, 1.6003, 1.6002, 1.5004, 1.5003r, 1.5, 1.5002 1.5003	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists in 'msg.asp' due to an input validation error, which could let a remote malicious user execute arbitrary code; a vulnerability exists in 'Login.ASP,' which could let a remote malicious user bypass the authentication system and obtain administrative access; and a vulnerability exists which could let a remote malicious user obtain sensitive information.	The vendor has stated that they are not able to reproduce this issue, but have released a Security Alert, 07/06/2003, that advises users on how to strengthen the overall security of the allegedly affected area of the product available at: http://www.earlyimpact.com/productcart/support/security-alert-070603.asp	ProductCart Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed or adminis-trative access can be obtained)**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.

[32] Secunia Security Advisory, July 1, 2003.
[33] Debian Security Advisory, DSA 343-1, July 8, 2003.
[34] Debian Security Advisory, DSA 339-1, July 6, 2003.
[35] Debian Security Advisory, DSA 340-1, July 6, 2003.
[36] NTBugtraq, July 2, 2003.
[37] 1ndonesian Security Team (1st) Security Advisory, July 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
GameSpy Industries [38]	Windows NT	Roger Wilco Mark 1d3	Two vulnerabilities exist: a buffer overflow vulnerability exists due to insufficient bounds checking before copying nicknames into memory, which could let a remote malicious user execute code; and a remote Denial of Service vulnerability exists when a malicious user submits a partial 'join-packet' instead of a full one.	Upgrade available at: http://rogerwilco.gamespy.com/products/downloads/rw_win_dload.html	Roger Wilco Remote Nickname Buffer Overflow & Denial of Service	LowHigh (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit script has been published for the buffer overflow vulnerability. Proof of Concept exploit has been published for the Denial of Service.
GNU[39]	Unix	AN	A buffer overflow vulnerability exists due to insufficient boundary checking on commandline options, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	GNU AN Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
GNU[40]	Unix	Chess 5.0 6, 5.0 5, 5.0 3beta, 5.0 2	A buffer overflow vulnerability exists due to insufficient bounds checking on commandline options, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	GNU Chess Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
GTKSee[41]	Unix	GTKSee 0.5.1 GTKSee 0.5.0	A vulnerability exists when PNG files that contain a certain color depth are loaded, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://developer.berlios.de/project/showfiles.php?group_id=735&release_id=1059 **Debian:** http://security.debian.org/pool/updates/main/g/gtksee/	GTKSee PNG Image Loading CVE Name: CAN-2003-0444	High	Bug discussed in newsgroups and websites.
Hewlett Packard Company [42]	Unix	Compaq Tru64 5.1b, PK1 (BL1), Tru64 5.1a, PK4 (BL21), PK3 (BL3), PK2 (BL2), PK1 (BL1), 5.1, PK6 (BL20), PK5 (BL19), PK4 (BL18), PK3 (BL17)	A Denial of Service vulnerability exists because KSH insufficiently terminates if a Telnet session is aborted abruptly.	Patches available at: http://ftp.support.compaq.com/patches/public/unix/v5.1/	Tru64 KSH Denial of Service	Low.	Bug discussed in newsgroups and websites.

[38] Securiteam, July 2, 2003.
[39] Securiteam, July 8, 2003.
[40] SecurityFocus, July 3, 2003.
[41] Debian Security Advisory, DSA 337-1, June 29, 2003.
[42] SecurityTracker Alert ID, 1007071, June 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company [43]	Multiple	NonStop SeeView Server Gateway G01.00, G02.00, G03.00, G04.00, G05.00, G05.01, G06.00, G06.01, G06.03-G06.20, D40.00, D41.00, D42.00, D42.01, D43.00-D43.02, D44.00-D44.02, D45.00, D45.01, D46.00, D47.00, D48.00-D48.03,	A vulnerability exists which could let a malicious user obtain elevated privileges.	Install T8488D40 AAC (HP SeeView Server Gateway) and T6965D40 AAF (HP SeeView Kernal) available at: http://www.support.compaq.com/patches/	NonStop SeeView Server Gateway Elevated Privileges CVE Name: CAN-2003-0458	Medium	Bug discussed in newsgroups and websites.
IglooFTP [44]	Windows	IglooFTP PRO 3.8	Multiple buffer overflow vulnerabilities exist due to insufficient checking performed on data that is copied into a reserved internal memory buffer, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.iglooftp.com/windows/IFTPPro39.exe	IglooFTP PRO Multiple Buffer Overflows	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Image Magick [45, 46]	Unix	Image Magick 5.4.4 .5	A vulnerability exists in the 'libmagick' library because temporary files are created insecurely, which could let a malicious user obtain elevated privileges.	**Debian:** http://security.debian.org/pool/updates/main/i/imagemagick/ **OpenPKG:** ftp://ftp.openpkg.org/	ImageMagick Insecure File Creation CVE Name: CAN-2003-0455	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Inktomi Corporation [47]	Multiple	Inktomi Search 5.0	A vulnerability exists when a malformed HTTP requests is submitted, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Inktomi Search Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[43] Hewlett-Packard Company Security Bulletin, SRB0084W, July 1, 2003.
[44] SecurityTracker Alert, 1007114, July 7, 2003.
[45] Debian Security Advisory, DSA 331-1, June 27, 2003.
[46] OpenPKG Security Advisory, OpenPKG-SA-2003.034, July 10, 2003.
[47] SecurityFocus, June 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Inter Systems Corpora-tion [48]	Unix	Cache 4.1.15, 5.0, 5.0.1, 5.0.2	A vulnerability exists due to insecure permissions on the content in the 'bin' and 'csp' directories, which could let a malicious user execute arbitrary code with root privileges.	No workaround or patch available at time of publishing.	InterSystems Cache Root Access CVE Name: CAN-2003-0497	**High**	Bug discussed in newsgroups and websites. There is no exploit code required however an exploit script has been published.
isdnrep[49]	Unix	isdnrep 4.56	A buffer overflow vulnerability exits due to insufficient bounds checking of data that is copied into a reserved internal memory buffer, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	ISDNRep Command Line Argument Local Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Joe Rumsey[50]	Unix	xgalaga 2.0.34	Several buffer overflow vulnerabilities exist due to a boundary error in the handling of the HOME environment variable, which could let a malicious user execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/x/xgalaga/	XGalaga Multiple Buffer Overflows CVE Name: CAN-2003-0454	**High**	Bug discussed in newsgroups and websites.
KDE[51] ***Conectiva issues advisory[52]***	**Unix**	**kopete 0.6.1**	**A vulnerability exists in the GnuPG plugin due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary commands.**	**Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br/**	**Kopete GnuPG Plugin Remote Command Execution** **CVE Name: CAN-2003-0256**	**High**	**Bug discussed in newsgroups and websites.**
Knoppix[53]	Multiple	Knoppix 3.1	A vulnerability exists because the 'knx-hdinstall; default configuration creates unsafe temporary files, which could let a malicious user cause a Denial of Service and potentially obtain elevated privileges.	No workaround or patch available at time of publishing.	Knoppix QT Insecure Temporary File Creation	Low/ Medium (Medium if elevated privileges can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.
Laforge Groups[54]	Windows, Unix	Forum51 2.5 b, 2.6 b	Several information disclosure vulnerabilities exist because the password file in not adequately protected, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Laforge Groups Forum51 Information Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[48] iDEFENSE Security Advisory, July 1, 2003.
[49] Securiteam, July 8, 2003.
[50] Debian Security Advisory, DSA 334-1, June 28, 2003.
[51] Mandrake Linux Security Update Advisory, MDKSA-2003:055, May 8, 2003.
[52] Conectiva Linux Security Announcement, CLA-2003:665, June 27, 2003.
[53] Bugtraq, July 8, 2003.
[54] Theblacksheep&erik Security Advisory, July 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Liece[55]	Unix	Liece 2.0	A vulnerability exists due to insufficient security precautions when creating temporary files, which could let a malicious user obtain elevated privileges.	Upgrade available at: http://security.debian.org/pool/updates/main/l/liece/	Liece Insecure Temporary File Creation	Medium	Bug discussed in newsgroups and websites.
Macromedia[56]	Windows NT 4.0/2000, XP	ColdFusion Server MX Profes-sional, Enterprise, Developer, 6.0	Several vulnerabilities exist: a vulnerability exists in the RDS service due to the way authentication is handled, which could let a remote unauthorized malicious user obtain access; a vulnerability exists because the RDS service uses a null password for authentication, which could let a remote unauthorized malicious user obtain access; a vulnerability exists because the RDS password is transmitted over the network in plain text, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because 'ASP SESSION IDs' are not validated, which could let a remote malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	ColdFusion Server MX Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploit script has been published for the RDS authentication vulnerability. There is no exploit code required for the null password vulnerability.
Macro-media[57]	Windows 95/98/NT 4.0/2000, Unix	ColdFusion Server MX Profes-sional, Enterprise, Developer, JRun 3.0, 3.1, 4.0, SP1&SP1a	A source disclosure vulnerability exists which could let an unauthorized malicious user obtain sensitive information.	Patches available at: http://download.macromedia.com/pub/security/mpsb03-04.zip	Macromedia Apache Web Server Encoded Space Source Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Mantis[58]	Unix	Mantis 0.17.1	A vulnerability exists due to weak permissions on the configuration file, which could let a malicious user obtain sensitive information.	**Debian:** http://security.debian.org/pool/updates/main/m/mantis/	Mantis Weak Configuration File Permission	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Marbry Software[59]	Windows NT	FTPServer/X 1.0.45, X 1.0.46; Mollensoft Software Hyperion FTP Server 3.5.2	A buffer overflow vulnerability exists in the wsprintf() function call due to insufficient bounds checking, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	Upgrade available at: http://www.mabry.com/ftpserv/index.htm	FTPServer/X Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.

[55] Debian Security Advisory, DSA 341-1, July 7, 2003.
[56] AngryPacket Security Advisory, June 26, 2003.
[57] Macromedia Security Advisory, MPSB03-04, July 8, 2003.
[58] Debian Security Advisory, DSA 335-1, June 28, 2003.
[59] Secunia Research Advisory, June 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Marut Deligonul [60]	Unix	ezbounce 1.0.4 a, 1.5 pre6	A format string vulnerability exists in the 'sessions' command, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	ezbounce Format String	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Mega Book[61]	Multiple	MegaBook 1.1, 2.0	Multiple Cross-Site Scripting vulnerabilities exist due to insufficient sanitization of HTML and script code from user-supplied input, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	MegaBook Multiple Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft [62]	Windows 2000	2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server SP1-SP3	A vulnerability exists due to a validation error in the way the Utility Manager handles Windows messages, which could let a malicious user obtain elevated privileges.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-025.asp	Windows Accessibility Utility Manager Privilege Escalation CVE Name: CAN-2003-0350	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft [63]	Windows 2000	Commerce Server 2002	A vulnerability exists in the 'HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\ Commerce Server' registry key if authentication has been configured to SQL Server authentication, which could let a malicious user obtain sensitive information.	It is reported that Microsoft will not be releasing a patch for this issue but will be releasing a Knowledge Base article addressing the issue.	Commerce Server 2002 Weak Registry Key Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft [64]	Windows NT 4.0/2000	Exchange Server 5.5, SP1-SP4, Exchange Server 2000, SP1&SP2	A Cross-Site Scripting vulnerability exists in Outlook Web Access (OWA) when e-mail messages are processed that contain HTML attachments, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Outlook Web Access Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites.

[60] Bugtraq, July 1, 2003.
[61] Exploitlabs.com Advisory, EXPL-A-2003-011, June 30, 2003.
[62] Microsoft Security Bulletin, MS03-025 V1.1, July 10, 2003.
[63] SecurityTracker Alert ID, 1007098, July 3, 2003.
[64] Secunia Security Advisory, July 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [65]	Multiple	URLScan 2.5	A vulnerability exists because IIS server HTTP header information can be exposed (even if the 'RemoveServerHeader' setting is enabled), which could let a remote malicious user obtain bypass security restrictions and obtain sensitive information.	No workaround or patch available at time of publishing.	URLScan Tool Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft [66]	Windows NT 4.0/2000, XP	Windows 2000 Terminal Services, SP1-SP3	A vulnerability exists because Kerberos ticketing is not handled properly, which could let a malicious user create a Kerberos ticket with two authorization data entries.	Upgrade available at: http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp	Windows Terminal Service Kerberos Ticket	Medium	Bug discussed in newsgroups and websites.
Microsoft [67]	Windows 2000, XP	Windows 2000 Advanced Server SP4, 2000 Datacenter Server SP4, 2000 Profes-sional SP4, 2000 Server SP4, XP Home SP1, XP Profes-sional SP1	A buffer overflow vulnerability exists in 'rundll32.exe' when a big string is submitted as a routine name for a module, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Windows 'RunDLL32. EXE' Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft [68]	Windows 2000	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3	A vulnerability exists in USBH_IoctlGetNode ConnectionDriverKeyName(), which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp	Windows 2000 USBH_Ioctl GetNode Connection DriverKey Name Information Disclosure	Medium	Bug discussed in newsgroups and websites.

[65] Secunia Security Advisory, July 7, 2003.
[66] Microsoft Service Pack 4 Announcement, June 26, 2003.
[67] Bugtraq, July 6, 2003.
[68] Microsoft Service Pack 4 Announcement, June 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [69]	Windows 2000	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3	A vulnerability exists in the 'MyGetSidFromDomain' function, which could let a malicious user spoof the domain controller.	Upgrade available at: http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp	Windows 2000 'MyGetSid FromDomain' Function	Medium	Bug discussed in newsgroups and websites.
Microsoft [70]	Windows 2000	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3	A buffer overflow vulnerability exists in the 'IMAADPCM' audio compression/decompression driver due to insufficient bounds checking, which could let a remote malicious user execute arbitrary instructions.	Upgrade available at: http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp	Windows IMAADPCM Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Microsoft [71]	Windows 2000	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Server, SP1-SP3	A Denial of Service vulnerability exists when the LDP tool is used to request a GUID.	Upgrade available at: http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp	Windows 2000 LDP Tool Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[69] Microsoft Service Pack 4 Announcement, June 26, 2003.
[70] Microsoft Service Pack 4 Announcement, June 26, 2003.
[71] Microsoft Service Pack 4 Announcement, June 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [72]	Windows 2000	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3	A buffer overflow vulnerability exists in API 'Port Name' due to the use of hard coded buffer sizes, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp	Windows 2000 Port Name Buffers Potential Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Microsoft [73]	Windows 2000	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3	A Denial of Service vulnerability exists in the Security Accounts Manager (SAM).	Upgrade available at: http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp	Windows Security Accounts Manager Denial of Service	Low	Bug discussed in newsgroups and websites.
Microsoft [74]	Windows 2000	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3	A buffer overflow vulnerability exists in the ShellExecute() API when an unusually long string is passed to the third string, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code.	Upgrade available at: http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp	Windows 2000 ShellExecute() Buffer Overflow Vulnerability	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[72] Microsoft Service Pack 4 Announcement, June 26, 2003.
[73] Microsoft Service Pack 4 Announcement, June 26, 2003.
[74] SNS Advisory No.65, July 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [75]	Windows 2000	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3	A vulnerability exists in 'cryptnet.dll' when dealing with LDAP sockets, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp	Windows 2000 Unspecified Cryptnet.DLL Memory Leakage Vulnerability	Medium	Bug discussed in newsgroups and websites.
Microsoft [76]	Windows 2000	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3	A vulnerability exists because a malicious WebBot can be loaded from a folder that is not under the global or version-specific WebBot folder on Microsoft IIS 5, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp	IIS _VTI_BOT Malicious WebBot	**High**	Bug discussed in newsgroups and websites.
Microsoft [77]	Windows 2000	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Server, SP1-SP3	A vulnerability exists in Active Directory Forests because a malicious user who is part of a trusted forest may enroll a certificate in a remote forest that they don't belong to.	Upgrade available at: http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp	Windows 2000 Active Directory Forest Origin Validation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[75] Microsoft Service Pack 4 Announcement, June 26, 2003.
[76] Microsoft Service Pack 4 Announcement, June 26, 2003.
[77] Microsoft Service Pack 4 Announcement, June 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [78]	Windows 2000	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3	A vulnerability exists when Internet Explorer is configured with 'Medium-Low' security settings, which could let a malicious user obtain unauthorized access.	Upgrades available at: http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp	Windows 2000 Unauthorized Access	Medium	Bug discussed in newsgroups and websites.
Microsoft [79]	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3	A vulnerability exists because named pipes are not properly handled through the 'CreateFile' API, which could let a malicious user obtain elevated privileges.	Upgrade available at: http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp	Windows CreateFile API Named Pipe Privilege Escalation CVE Name: CAN-2003-0496	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft [80] ***Exploit script has been published*** [81]	**Windows 2000**	**Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1- SP4, 2000 Server, SP1- SP4**	**A buffer overflow vulnerability exists in the way 'nsiislog.dll' processes incoming client requests, which could let a remote malicious user execute arbitrary code.**	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-022.asp**	**Windows Media Services NSIISlog.DLL Remote Buffer Overflow CVE Name: CAN-2003-0349**	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published.**

[78] Microsoft Service Pack 4 Announcement, June 26, 2003.
[79] @stake, Inc. Security Advisory, July 8, 2003.
[80] Microsoft Security Bulletin, MS03-022, June 25, 2003.
[81] SecurityFocus, July 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [82]	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Work-station 4.0, SP1-SP6a, XP 64-bit Edition, SP1, XP Home, SP1, XP Profes-sional, SP1	A buffer overflow vulnerability exists in the Server Message Block (SMB) packet due to insufficient validation, which could let a malicious user cause a Denial of Service or execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-024.asp	Microsoft SMB Request Handler Buffer Overflow CVE Name: CAN-2003-0345	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft [83] ***Exploit script has been published*** [84]	**Windows 2000**	**Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1- SP4, 2000 Server, SP1- SP4**	**A buffer overflow vulnerability exists in the way 'nsiislog.dll' processes incoming client requests, which could let a remote malicious user execute arbitrary code.**	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-022.asp**	**Windows Media Services NSIISlog.DLL Remote Buffer Overflow CVE Name: CAN-2003-0349**	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published.**

[82] Microsoft Security Bulletin, MS03-024V1.1, July 10, 2003
[83] Microsoft Security Bulletin, MS03-022, June 25, 2003.
[84] SecurityFocus, July 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [85]	Windows 95/98/ME/ NT 4.0/2000, XP, 2003	Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1-SP4, 2000 Profes-sional, SP1-SP4, 2000 Server, SP1-SP4, Windows 98/SE/ME, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Work-station 4.0, SP1-SP6a, Windows Server 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, XP 64-bit Edition, SP1, XP Home, XP Media Center Edition, XP Profes-sional, SP1	A buffer overflow vulnerability exists due to the way the HTML converter handles conversion requests during a cut-and-paste operation, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-023.asp	Windows HTML Converter Buffer Overflow CVE Name: CAN-2003-0469	**High**	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the press and other public media.

[85] Microsoft Security Bulletin, MS03-023 V1.2, July 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[86] ***Microsoft updates bulletin***[87]	**Windows 95/98/ME/ NT 4.0/2000, XP, 2003**	**Windows Media Player 9.0**	**A vulnerability exists due to insufficient validation of requests made to the ActiveX control, which could let a malicious user obtain sensitive information.** ***Bulletin updated to reflect the corrected registry key for verification of patch install.***	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-021.asp**	**Media Player 9 Unauthorized Media Library Access** **CVE Name: CAN-2003-0348**	**Medium**	**Bug discussed in newsgroups and websites.**
Mike Bryeans[88]	Windows, Unix	WebBBS Pro 1.18	A Cross-Site Scripting vulnerability exists due to missing validation of user input supplied in various fields ("Name," "Email," and "Message") when signing the guest book, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	WebBBS Guestbook Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Miquel van Smooren-burg[89, 90] ***Conectiva issues advisory***[91]	**Unix**	**Cistron Radius 1.6.4-1.6.6**	**A buffer overflow vulnerability exists when a long specially crafted NAS-Port attribute is submitted, which could let a remote malicious user execute arbitrary code.**	**SuSE: ftp://ftp.suse.com/pub/suse/** **Debian: http://security.debian.org/pool/updates/main/r/radiusd-cistron/** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br/**	**Cistron RADIUS Buffer Overflow NAS-Port Attribute**	**High**	**Bug discussed in newsgroups and websites.**
Mirabilis[92]	Windows	ICQ 2003 a Build 3800, 3799, 3777	A vulnerability exists due to an authentication error, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	ICQ Password Bypass	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
more groupware[93]	Windows, Unix	moregroup ware 0.6.7	Several Cross-Site Scripting vulnerabilities exist due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	MoreGroup Ware Multiple Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.

[86] Microsoft Security Bulletin, MS03-021, June 25, 2003.
[87] Microsoft Security Bulletin, MS03-021 V1.1, July 4, 2003.
[88] Bugtraq, June 27, 2003.
[89] SuSE Security Announcement, SuSE-SA:2003:030, June 13, 2003.
[90] Debian Security Advisory, DSA 321-1, June 13, 2003.
[91] Conectiva Linux Security Announcement, CLA-2003:664, June 27, 2003.
[92] Bugtraq, July 5, 2003.
[93] Security Corporation Advisory, KSA-002, June 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
more groupware [94]	Windows, Unix	moregroup ware 0.6.7	A vulnerability exists which could let a remote malicious user upload and possibly overwrite arbitrary files.	No workaround or patch available at time of publishing.	MoreGroup Ware Arbitrary File Upload	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Mozart[95]	Unix	Mozart 1.2.3, 1.2.5	A vulnerability exists in the mailcap configuration file, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://security.debian.org/pool/updates/main/m/mozart/	Mozart Mailcap Configuration	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
MRV Commun-ications, Inc.[96] ***Vendor's response[97]***	**Multiple**	**OptiSwitch 800, 400**	**A vulnerability exists when a specific sequence of key presses is initiated, which could let a remote malicious user obtain root access.** ***The vendor has responded and has reported that this vulnerability does not exist.***	**No workaround or patch available at time of publishing.**	**OptiSwitch 400/800 Unauthorized Remote Root Access**	**High**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Multiple Vendors[98]	Unix	Linux kernel 2.4-2.4.21	A vulnerability exits due to an error in the "execve()" system call when handling the file descriptor for the target executable, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Linux 2.4 Kernel execve() System Call Race Condition	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Multiple Vendors [99, 100, 101] ***More vendors release advisories*** [102, 103]	**Unix**	**Adobe Acrobat Reader (UNIX) 5.06; RedHat Linux 7.1, 7.2 ia64, i386, 7.3 i386, 8.0 i386, 9.0 i386; Xpdf Xpdf 0.92, 1.0, 1.0 1, 2.0, 2.0.1**	**A vulnerability exists when hyperlinks have been enabled within the PDF viewer, which could let a remote malicious user execute arbitrary shell commands.**	**YellowDog:** ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/ppc/ **RedHat:** ftp://updates.redhat.com/ ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php ***Conectiva:*** ftp://atualizacoes.conectiva.com.br/	**Multiple Vendor PDF Hyperlinks** **CVE Name: CAN-2003-0434**	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published.**

[94] Security Corporation Advisory, KSA-002, June 26, 2003.
[95] Debian Security Advisory, DSA 342-1, July 7, 2003.
[96] Bugtraq, June 25, 2003.
[97] SecurityFocus, July 2, 2003.
[98] Bugtraq, June 26, 2003.
[99] Red Hat Security Advisory, RHSA-2003:196-01, June 18, 2003.
[100] Yellow Dog Linux Security Announcement, YDU-20030620-1, June 20, 2003.
[101] Turbolinux Security Advisory, TLSA-2003-39, June 24, 2003.
[102] Mandrake Linux Security Update Advisory, MDKSA-2003:071, June 27, 2003.
[103] Conectiva Linux Security Announcement, CLA-2003:674, July 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [104, 105, 106, 107]	Unix	Mandrake Soft Corporate Server 2.1, Linux Mandrake 8.2, ppc, 9.0; Terra Soft Solutions Yellow Dog Linux 2.3, 3.0; ypserv ypserv 1.3.11, 1.3.12, 2.2, 2.5-2.7	A Denial of Service vulnerability exists in the Network Information Service (NIS) server when a malicious user queries ypserv via TCP and subsequently ignores the server's response.	**Ypserv:** ftp://ftp.kernel.org/pub/linux/utils/net/NIS/ypserv-2.8.tar.gz **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **RedHat:** ftp://updates.redhat.com/ **Sun:** http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F55600 **YellowDog:** ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/	Multiple Vendor YPSERV Denial of Service CVE Name: CAN-2003-0251	Low	Bug discussed in newsgroups and websites.
myServer [108]	Windows, Unix	myServer 0.4.2	A remote Denial of Service vulnerability exists when handling certain malformed URIs.	No workaround or patch available at time of publishing.	MyServer Malformed URI Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploits have been published.
NetScreen Technologies [109]	Multiple	ScreenOS 3.x, 4.x	A vulnerability exists when operating in Bridge Mode because any non-IP or ARP traffic will bypass the firewall without being logged, which could let a remote malicious user bypass security restrictions.	The vendor plans to issue maintenance releases to ScreenOS 4.0.1 and 4.0.3 the week of July 14.	NetScreen Non-IP Traffic Firewall Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
NGC [110]	Windows NT	Active MailServer 2002	A buffer overflow vulnerability exists because the SMTP service doesn't handle long arguments to the 'HELO,' 'MAIL FROM.' and 'RCPT TO' parameters correctly, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Active MailServer SMTP Command Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Nik Reiman [111]	Unix	Portmon 1.0-1.8	A buffer overflow vulnerability exists in the 'USER' environment variable due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	Upgrade available at: http://aboleo.net/software/portmon/downloads	Portmon 'USER' Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[104] Red Hat Security Advisory RHSA-2003:173-01, June 25, 2003.
[105] Mandrake Linux Security Update Advisory, MDKSA-2003:072, June 27, 2003.
[106] Yellow Dog Linux Security Announcement, YDU-20030627-1, June 27, 2003.
[107] Sun(sm) Alert Notification, 55600, July 2, 2003.
[108] Exploitlabs.com, EXPL-A-2003-012, July 6, 2003.
[109] SecurityTracker Alert ID, 1007148, July 9, 2003.
[110] SecurityFocus, June 26, 2003.
[111] Bugtraq, June 25, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Novell[112]	Multiple	iChain Server 2.2, 2.2 FP1a&FP1	Multiple vulnerabilities exist that could let an unauthorized malicious user obtain sensitive information or redirect clients to a malicious website.	Upgrade available at: http://support.novell.com/servlet/filedownload/sec/pub/ic22sp1.exe	iChain Server Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Open LDAP[113] ***Conectiva issues advisory*** [114]	**Unix**	**OpenLDAP 2.0-2.0.23, 2.0.25, 2.0.27, 2.1.10-2.1.16**	**A remote Denial of Service vulnerability exists when the server attempts to free an uninitialized structure during authentication.**	**Upgrade available at: ftp://ftp.OpenLDAP.org/pub/OpenLDAP/openldap-release/openldap-2.1.20.tgz** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br**	**OpenLDAP Remote Denial of Service**	**Low**	**Bug discussed in newsgroups and websites.**
OpenBSD [115]	Unix	OpenBSD 3.0-3.2	A vulnerability exists when a packet filter is used to redirect incoming traffic from standard ports to a higher and nonprivileged port, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	OpenBSD Incoming Traffic Redirect	Medium	Bug discussed in newsgroups and websites. Vulnerability e can be exploited with a port scanner such as nmap. Proofs of Concept exploits have also been published.
Opera Software [116]	Windows	Opera Web Browser 7.0 3win32, 7.10, 7.11b, 7.11	Five Denial of Service vulnerabilities exist when the browser attempts to interpret a document that contains malformed code.	No workaround or patch available at time of publishing.	Multiple Opera Denial of Service	Low	Bug discussed in newsgroups and websites. Exploits have been published.
Palm[117]	Multiple	Palm OS 3.3, 3.5 h, 3.5.2, 4.0, 4.1, 5.0	A vulnerability exists due to insufficient protection on documents that have 'privacy' enabled, which could let a malicious user modify sensitive information.	No workaround or patch available at time of publishing.	PalmOS MemoPad Memo Hiding Bypass	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited with a third-party text editor.

[112] Novell Technical Information Document, TID2966435, July 8, 2003.
[113] SecurityFocus, May 22, 2003.
[114] Conectiva Linux Security Announcement, CLA-2003:685, July 4, 2003.
[115] Bugtraq, July 2, 2003.
[116] SecurityFocus, June 30, 2003.
[117] Bugtraq, July 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PHP Arena[118]	Windows, Unix	paBox 1.6	Several vulnerabilities exist: a vulnerability exists in the 'shoutbox/tagboard' script because administrative passwords may be reset, which could let an unauthorized remote malicious user obtain administrative access; and a vulnerability exists in the Administrative Control Panel when adding banned users, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PABox Password Reset & Administrative Control Panel	High	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser however an exploit has been published. There is no exploit code required for the administrative control panel vulnerability.
PHP Group Ware[119]	Windows, Unix	PHPGroup Ware 0.9.14 .003	Multiple Cross-Site Scripting vulnerabilities exist in the form fields due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Multiple PHPGroup Ware HTML Injection	High	Bug discussed in newsgroups and websites. There is no exploit code required.
phpBB Group[120] ***Vendor issues code modification-tion[121]***	**Windows, Unix**	**phpBB 2.0.0-2.0.4**	**A vulnerability exists in the 'theme_info.cfg' script, which could let a malicious user obtain sensitive information or execute arbitrary commands.**	***The vendor has addressed this issue by supplying a code modification in a post on their forum available at:*** **http://www.phpbb.com/phpBB/viewtopic.php?t=113826**	**PHPBB Theme_Info. CFG File Include**	**Medium/ High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
phpSys Info[122] ***Debian issues advisory[123]***	**Unix**	**phpSysInfo 2.1**	**A file disclosure vulnerability exists because the include path for several template files and language include files can be influenced, which could let a malicious user obtain sensitive information and execute arbitrary code.**	**No workaround or patch available at time of publishing.** ***Debian:*** **http://security.debian.org/pool/updates/main/p/phpsysinfo/**	**PHPSysInfo File Disclosures**	**Medium/ High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**

[118] Bugtraq, June 30, 2003.
[119] Kereval Security Advisory, KSA-003, July 2, 2003.
[120] SecurityFocus, June 16, 2003.
[121] SecurityFocus, June 26, 2003.
[122] SecurityFocus, April 4, 2003.
[123] Debian Security Advisory, DSA 346-1, July 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
phpSysInfo[124] ***Upgrade now available***[125] ***Debian issues advisory***[126]	**Unix**	**phpSysInfo 2.1**	**A file disclosure vulnerability exists because the include path for several template files and language include files can be influenced, which could let a malicious user obtain sensitive information and execute arbitrary code.**	***Upgrade available at:*** **http://cvs.sourceforge.net/cgi-bin/viewcvs.cgi/phpsysinfo/phpsysinfo-dev/index.php.diff?r1=1.56&r2=1.57** ***Debian:*** **http://security.debian.org/pool/updates/main/p/phpsysinfo/**	**phpSysInfo File Disclosures**	**Medium/ High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
Pierre Chifflier[127]	Unix	wzdftpd 0.1, 0.1 rc4	A remote Denial of Service vulnerability exists when a malicious user submits an incomplete or malformed FTP PORT command.	Upgrade available at: http://www.wzdftpd.net/download.html	WZDFTPD Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability can be exploited with an FTP client.
ProFTPD Project[128] ***Debian issues advisory***[129]	**Unix**	**ProFTPD 1.2 pre1-pre11, 1.2.0rc1-1.2.0rc3, 1.2-1.2.9 rc1**	**A vulnerability exists in versions that that use the mod_sql module to manipulate PostgreSQL databases due to insufficient sanitization of user-supplied data when logging onto the server, which could let a remote malicious user execute arbitrary code.**	***Debian:*** **http://security.debian.org/pool/updates/main/p/proftpd/**	**ProFTPD 'mod_sql' Module**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.**
Quad Comm, Inc.[130]	Windows	Q-Shop 2.5	A vulnerability exists due to insufficient authentication validation, which could let a remote malicious user execute arbitrary script.	No workaround or patch available at time of publishing.	Q-Shop Credential Validation	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser, however, an exploit script has been published.
Rockliffe[131]	Windows NT 4.0/2000	MailSite 5.3.4	A vulnerability exists because attachments are stored in the 'cache' directory when requests are authenticated, which could let a remote malicious user view attachments stored on the server.	No workaround or patch available at time of publishing.	Mailsite Attachment Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[124] SecurityFocus, April 4, 2003.
[125] SecurityFocus, April 25, 2003.
[126] Debian Security Advisory, DSA 346-1, July 8, 2003.
[127] Secunia Security Advisory, June 30, 2003.
[128] Securiteam, June 19, 2003.
[129] Debian Security Advisory, DSA-338-1, June 29, 2003.
[130] Zone-h Security Team Security Advisory, ZH2003-2SA, July 10, 2003.
[131] Zone-h Security Team Advisory, ZH2003-1SA, July 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sam Lantinga [132] ***Exploit script published*** [133]	**Unix**	**Maelstrom 3.0.3, 3.0.5, 3.0.6**	**A buffer overflow vulnerability exists due to insufficient bounds checking of user-supplied data, which could let a malicious user execute arbitrary code.**	**No workaround or patch available at time of publishing.**	**Maelstrom Server & Player Argument Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.** ***Exploit scripts have been published.***
SSH Communications Security [134]	Windows, Unix	IPSEC Express Toolkit 5.0.0, SSH2 3.1-3.1.7, 3.2- 3.2.4	A vulnerability exists because certain RSA signatures might be incorrectly verified, which could let a remote malicious user forge RSA signatures.	Upgrades available at: http://www.ssh.com/support/downloads/	Secure Shell/IPSEC Express Toolkit RSA Signature Forging	Medium	Bug discussed in newsgroups and websites.
Sun Microsystems, Inc.[135]	Unix	Solaris 2.5.1, 2.6, 7.0, 8.0, 9.0; Veritas File System 3.3.3, 3.4, 3.5	A vulnerability exits in the VERITAS File System (VxFS) files due to incorrect permissions being set when Access Control Lists (ACLs) are utilized, which could let a malicious user obtain sensitive information.	Patches available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F55060	Solaris Veritas File System Incorrect File Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Microsystems, Inc.[136]	Unix	Solaris 8.0_x86, 8.0	A vulnerability exists when a deadlock condition is created and the system is under a heavy load, which could let a malicious user cause the system to crash.	Patches available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F53584	Solaris Deadlock Condition	Low	Bug discussed in newsgroups and websites.
Symantec [137]	Windows XP	Norton AntiVirus Corporate Edition 7.60.build 926	A vulnerability exists in NAVCE (specifically on Windows XP systems) due to a failure to scan floppy disks for malicious code, which could let a malicious user execute arbitrary code.	Affected customers are advised to contact the vendor for details regarding updates.	Symantec NAVCE Floppy Disk Scan Failure	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
teapop[138]	Unix	teapop 0.3.4, 0.3.5	A vulnerability exists due to input validation errors in modules included for authenticating against a PostgreSQL or MySQL database, which could let a remote malicious user obtain sensitive information or manipulate data.	Upgrades available at: http://security.debian.org/pool/updates/main/t/teapop/	Teapop Authentication Modules CVE Name: CAN-2003-0515	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[132] Bugtraq, May 18, 2003.
[133] SecurityFocus, July 9, 2003.
[134] SecurityTracker Alert, 1007086, June 30, 2003.
[135] Sun(sm) Alert Notification, 55060, June 27, 2003.
[136] Sun(sm) Alert Notification, 53584, June 26, 2003.
[137] Bugtraq, June 27, 2003.
[138] Debian Security Advisory, DSA 347-1, July 8, 2003

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Tower Toppler[139]	Multiple	Tower Toppler 0.96	A buffer overflow vulnerability exists in the 'HOME' environment variable, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Tower Toppler Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Unreal[140]	Multiple	Unreal IRCd 3.1.1, 3.1.3, 3.2 .0 beta 10	A Denial of Service vulnerability exists in 'operserv' when a malicious client submits a raw message to a nonexistent nick or a raw message is used when requesting to join a channel.	No workaround or patch available at time of publishing.	Unreal IRCD Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Verity Inc.[141]	Windows, Unix	K2 Toolkit 2.20	A Cross-Site Scripting vulnerability exists due to an input validation error in Query Builder when displaying error messages, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	Verity K2 Toolkit Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
VMWare, Inc.[142]	Unix	VMWare Work-station 4.0	A vulnerability exists because files are created insecurely in "/tmp" if "TMPDIR" hasn't been specified, which could let a malicious user obtain elevated privileges.	**Workaround:** The vendor has reported that it is possible to implement a workaround for this issue, by setting the TEMPDIR environment variable in a way such that temporary files are created in a secure location.	VMware Workstation 4.0 Insecure Temporary	Medium	Bug discussed in newsgroups and websites.
XBlock Out[143]	Unix	xbl 1.0k, 1.0i	A buffer overflow vulnerability exists in the '-display' commandline option due to a boundary error, which could let a malicious user execute arbitrary code.	Upgrades available at: http://security.debian.org/pool/updates/main/x/xbl/	XBlockOut Buffer Overflow CVE name: CAN-2003-0535	**High**	Bug discussed in newsgroups and websites.
XFree86[144] ***Conectiva issues advisory***[145]	**Unix**	**X11R6 4.2.0, 4.2.1**	**A buffer overflow vulnerability exists due to the way the 'XLOCALEDIR' string is handled, which could let a malicious user execute arbitrary code.**	***Conectiva:*** **ftp://ul.conectiva.com.br/updates/**	**XFree86 XLOCALE DIR Local Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.**

[139] Securiteam, July 8, 2003.
[140] SecurityFocus, July 8, 2003.
[141] Securiteam, July 3, 2003.
[142] Securiteam, July 1, 2003.
[143] Debian Security Advisory, DSA 345-1, July 8, 2003.
[144] Securiteam, March 7, 2003.
[145] Conectiva Linux Security Announcement, CLSA-2003:682, July 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
zkfingerd [146]	Unix	zkfingerd 0.9.1, 2.0.1, 2.0.2	A format string vulnerability exists in the _finger_error() function, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	ZKFingerD Format String	High	Bug discussed in newsgroups and websites.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between June 26 and July 11, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 41 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Script Description
July 11, 2003	DSR-mnogo.pl	Proof of concept exploit for mnoGoSearch 3.1.20 vulnerability.
July 11, 2003	Shatter_Redux.pdf	Security paper that reflects on the Shatter Attacks found against the Windows operating system in 2002.
July 10, 2003	**bosen.asp**	**Exploit for the Q-Shop Credential Validation Vulnerability.**
July 9, 2003	**acroread-poc.pl**	**Perl script that exploits the Adobe Unix Acrobat Reader Buffer Overflow vulnerability.**
July 9, 2003	**ccbillx.c**	**Script that exploits the CCBill WhereAmI.cgi Script vulnerability.**
July 9, 2003	**DSR-listproc.pl**	**Perl script that exploits the ListProc ULISTPROC_UMASK Buffer Overflow vulnerability.**
July 9, 2003	**MaelstromX.c**	**Script that exploits the Maelstrom Server & Player Argument Buffer Overflow vulnerability.**

[146] Ph4nt0m Security Advisory 2#2003--7-7, July 8, 2003.

Date of Script (Reverse Chronological Order)	Script name	Script Description
July 9, 2003	**maelx.pl**	**Script that exploits the Maelstrom Server & Player Argument Buffer Overflow vulnerability.**
July 9, 2003	xfocus-nsiislog-exploit.c	Script that exploits the Windows Media Services NSIISlog.DLL Remote Buffer Overflow vulnerability.
July 8, 2003	**5358gnuanx0r.c**	**Script that exploits the GNU AN Buffer Overflow vulnerability.**
July 8, 2003	**5358isdnrape.c**	**Script that exploits the ISDNRep Command Line Argument Local Buffer Overflow vulnerability.**
July 7, 2003	**FBHtoppler.c**	**Script that exploits the Tower Toppler Buffer Overflow vulnerability.**
July 7, 2003	fport.zip	A powerful windows tool which reports all open TCP/IP and UDP ports and maps them to the owning application.
July 7, 2003	**gkrellmail.c**	**Script that exploits the GKrellM Mailwatch Remote Buffer Overflow vulnerability.**
July 7, 2003	RpcScan101.zip	RpcScan enumerates the RPC endpoint-map elements for port 135.
July 6, 2003	connlogd-0.9.7.tar.gz	A detailed TCP/UDP connection logger with the ability to filter what information is logged.
July 6, 2003	DSR-ftp_clients.pl	This script runs in place of ftpd to exploit the moxftp/mftp 2.2, cftp 0.12, and Iglooftp 0.6.1 clients.
July 6, 2003	eXtremail.txt	Exploit for the Linux eXtremail Format String vulnerability.
July 6, 2003	eXtreme.c	Script that exploits the Linux eXtremail Format String vulnerability.
July 6, 2003	IglooFTPPRO.txt	Proof of Concept exploit for the IglooFTP PRO Multiple Buffer Overflows vulnerability.
July 6, 2003	iglooftppro.zip	Exploit for the IglooFTP PRO Multiple Buffer Overflows vulnerability.
July 6, 2003	path.tgz	A collection of hijacking tools that is written in Perl.
July 5, 2003	**ca1-icq.asm**	**Exploit for the ICQ Password Bypass vulnerability.**
July 5, 2003	disco-1.2.tar.gz	A passive IP discovery utility designed to sit on segments distributed throughout a network and discover unique IPs. In addition to IP discovery Disco has the ability to passively fingerprint TCP SYN packets to determine the host operating system.
July 4, 2003	essenexploit.c	Exploit for the Essentia Linux Webserver Buffer Overflow vulnerability.
July 4, 2003	wilco.zip	Exploit for the Roger Wilco Remote Nickname Buffer Overflow vulnerability.
July 3, 2003	**5358gchessfuck.c**	**Script that exploits the GNU Chess Buffer Overflow vulnerability.**
July 3, 2003	nessus-installer.sh	A free, up-to-date, and full featured remote vulnerability scanner for Linux, BSD, Solaris and other systems that is multithreaded, plugin-based, has a nice GTK interface, and currently performs over a thousand remote security checks. It has powerful reporting capabilities (HTML, LaTeX, ASCII text) and not only points out problems, but also suggests a solution for each of them.
July 2, 2003	**DSR-crapche.sh**	**Script that exploits the InterSystems Cache Root Access vulnerability.**
July 1, 2003	**xezb.c**	**Script that exploits the ezbounce Format String vulnerability.**

Date of Script (Reverse Chronological Order)	Script name	Script Description
June 29, 2003	art_of_brute_forcing.txt	Paper written about the art of brute force cracking that comes with example code.
June 29, 2003	DominoHunter-0.9.zip	A Lotus Domino web server scanner, written in Perl that attempts to access default NSF databases, as well as crawl user-defined bases. It tries to enumerate the database structure, enumerate available views, available documents, and ACLs set on documents.
June 29, 2003	**DSR-geekrellm-linux.pl**	**Script that exploits the GKrellM Mailwatch Remote Buffer Overflow vulnerability.**
June 29, 2003	**gkrhack0x03.c.gz**	**Script that exploits the GKrellM Mailwatch Remote Buffer Overflow vulnerability.**
June 29, 2003	login_hacker-1.1.tar.gz	THC Modem Login Hacker is a tool that will attempt to break into modem dialups using scripts written for minicom.
June 29, 2003	**poc505.pl**	**Perl script that exploits the Adobe Unix Acrobat Reader Buffer Overflow vulnerability.**
June 29, 2003	**poc507.pl**	**Perl script that exploits the Adobe Unix Acrobat Reader Buffer Overflow vulnerability.**
June 26, 2003	ircc.c	Script that exploits the Bahamut IRCd Remote Format String vulnerability.
June 26, 2003	**RDS_c_Dump.pl**	**Perl script that exploits the ColdFusion Server MX RDS authentication vulnerability.**
June 26, 2003	**suiddmp.c**	**Script that exploits the Linux 2.4 Kernel execve() System Call Race Condition vulnerability.**
June 26, 2003	test2.zip	Script that exploits the Windows HTML Converter Buffer Overflow vulnerability.

Trends

- **Recent reports to the CERT/CC have highlighted two chronic problems:**
  - **The speed at which viruses are spreading is increasing. This echoes the trend toward faster propagation rates seen in the past few years in self-propagating malicious code (i.e., worms). A similar trend from weeks to hours has emerged in the virus (i.e., non-self-propagating malicious code) arena.**
  - **In a number of the reports, users who were compromised may have been under the incorrect impression that merely having antivirus software installed was enough to protect them from all malicious code attacks. This is simply a mistaken assumption, and users must always exercise caution when handling e-mail attachments or other code or data from untrustworthy sources. For more information see, CERT® Incident Note IN-2003-01, located at: http://www.cert.org/incident_notes/IN-2003-01.html.**
- **The Fortnight Internet worm takes advantage of a the Microsoft VM ActiveX security vulnerability for which Microsoft released a security patch three years ago. When this security breach is left unpatched the worm's code is allowed to be executed on victim computers.**
- **A growing trend sees spammers targeting home computers with Trojan programs to remotely send out spam. Spammers are less likely to crack corporate boxes and are now increasingly turning toward using large quantities of home computers.**
- **The Department of Homeland Security has noticed an increase in the use of mass mailing techniques to distribute malicious code. Several recent forms of malicious code, such as the W32/Fizzer@MM Worm (see DHS Advisory 03-#023), variations of the Sobig virus (W32/Sobig-A, B and C), and BugBear (W32/BugBear A and B) were propagated via e-mail. For more information see: http://www.nipc.gov/publications/infobulletins/2003/MassMailingMalicious%20Code.htm.**
- **The underlying code for the Slammer worm is planned to be published by *Wired* magazine. The article, which will be published in Wired's July issue due out on Tuesday, details how the**

Slammer worm, also known as "SQL Slammer," spread rapidly through the Internet on Jan. 25, shutting down Internet service providers in South Korea, disrupting plane schedules and knocking out automatic teller machines.

- **According to new research, nearly three-quarters of malicious connections to wireless networks are used for sending spam. A survey found that almost a quarter of unauthorized connections to the wireless LANs were intentional, and 71 per cent of those were used to send e-mails.**
- **The number of security events detected by companies in the first quarter of 2003 jumped nearly 84 percent over the preceding three months. The increase in events, which can include minor probes for holes in network security as well as major attacks, stems mainly from an increase in worms and automated attack software.**

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Bugbear	File	Increase	September 2002
2	W32/Klez	Worm	Slight Decrease	January 2002
3	W32/Sobig	Worm	Increase	May 2003
4	W32/Yaha	Worm	Slight Decrease	February 2002
5	W32/Lovegate	Virus	Stable	February 2003
6	Funlove	File	Return to table	November 1999
7	JS/NoClose	Trojan	Increase	May 2002
8	Elkern	File Infector	Decrease	October 2001
9	W32/SQLSlammer	Worm	Stable	January 2003
10	W32/Fizzer	Worm	Decrease	May 2003

Note: Note: Virus reporting may be weeks behind the first discovery of infection. A total 212 distinct viruses are currently considered "in the wild" by anti-virus experts, with another 320 viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

VBS.Nuf.Worm (Visual Basic Script Worm): This is a script that an executable file drops or another Visual Basic script copies. When VBS.Nuf.Worm runs, it searches all the mapped drive letters. If the drive is a local or network hard drive, or an available removable drive, the worm copies itself to the root of the drive as Scriptfile.vbs. There is no other payload.

W32.Atendo@mm (Aliases: Trojan.Win32.Atendo, W32/Payfor@M): Win32 Worm): This is a worm that replies to all the e-mail messages it finds in the Microsoft Outlook Inbox of an infected computer. The worm also contains a destructive payload that deletes certain files from an infected computer.

W32/Colevo-A (Aliases: W32.Vivael@mm, I-Worm.Colevo, W32/Colevo@MM, WORM_COLEVO.A) (Win32 Worm): This is an e-mail worm that sends itself to the infected user's MSN Messenger contacts. The e-mail will have the following characteristics:

- Subject line: El fin se puede hackear a hotmail!!
- Attached file: hotmailpass.exe

W32/Colevo-A copies itself to various files and makes the following registry changes:

- HKCR\htafile\shell\open\command\(Default) = "C:\Windows\commands.exe", "%1 %*"
- HKCR\exefile\shell\open\command\(Default) = "C:\Windows\command.exe", "%1 %*"
- HKCR\comfile\shell\open\command\(Default) = "C:\Windows\Inf.exe", "%1 %*"
- HKCR\batfile\shell\open\command\(Default) = "C:\Windows\temp.exe", "%1 %*"
- HKCR\piffile\shell\open\command\(Default) = "C:\Windows\commands.exe", "%1 %*"
- HKCR\exefile\NeverShowExt
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\System = C:\Windows\system.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\1\2\3\4\System = C:\Windows\temp.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\System = C:\Windows\commands.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\System = C:\Windows\system.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\1\2\3\4\System = C:\Windows\system.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\System = C:\Windows\temp.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce\System = C:\Windows\system.exe

The file winstart.bat will be created and will contain the single line "null=c:\windows\system.exe." W32/Colevo-A runs in the background as a backdoor server allowing unauthorized access to the victim's computer. It continually opens the user's web browser to various links. All the links above contain clean image files.

W32/Graps-A (Aliases: W32/Graps.worm, W32.HLLW.Graps, Win32.Graps, Worm.Win32.Graps, Win32.Graps) (Win32 Worm): This is a worm that uses Windows hidden system shares, intended for inter process communication and administration tasks (IPC$ and ADMIN$), to spread. It spreads with the filename mwd.exe together with two other files, a utility psexec.exe and an OCX file mswinsck.ocx. The worm drops three batch files: wds.bat, wds2.bat, and wds3.bat into the current directory. The dropped batch files are used to probe for IPC$ or ADMIN$ shares with weak or blank passwords. If a share is successfully probed, the batch file copies wdm.exe, psexec.exe, and mswinsck.ocx to the remote computer and uses psexec.exe to remotely launch wdm.exe. W32/Graps-A creates a new registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Windows Management Instrumentation

so that the file wdm.exe from the Windows System folder is run on Windows startup. The worm also contains a backdoor component that can be used by a malicious user to launch Denial of Service attacks or use an infected machine as a TCP proxy.

W32.HLLW.Merkur.E@mm (Alias: I-Worm.Merkur.d) (Win32 Worm): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all the contacts in the Outlook Address Book. It also attempts to spread through the KaZaA, KaZaA Lite, Bearshare, and eDonkey file-sharing networks, as well as through mIRC. The e-mail message has the following characteristics:

- Subject: (one of the following)
  Free Virus Remover.
  Windows Update (Build: win1.19001281)
  Email Virus Remover.

- Attachment: AVUpdate.exe

This worm is written in the Microsoft Visual Basic programming language and is compressed with UPX.

W32.HLLW.Niden (Win32 Worm): This is a worm that attempts to spread itself through file-sharing networks. It also attempts to mass-mail itself to all the contacts in the Windows Address Book. However, due to bugs in the code, the mass-mailing routine does not work properly. Furthermore, it attempts to disguise itself as Norton Anti-Virus 2003 by using an icon. When W32.HLLW.Niden is executed, it displays a fake error message, titled "Error Starting Application." The worm also attempts to delete files belonging to various antivirus programs. W32.HLLW.Niden is written in the Microsoft Visual Basic (VB) programming language. The VB run-time libraries are required to execute W32.HLLW.Niden.

W32.HLLW.Redist.C@mm (Win32 Worm): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all the contacts in the Outlook Address Book. The worm also attempts to spread itself through KaZaA, KaZaA Lite, KMD, LimeWire, Gnucleus, Shareaza, BearShare, Edonkey, Edonkey2000, Morpheus, Grokster, WinMX, Tesla, Overnet, XoloX, Rapigator file-sharing networks, and ICQ. When W32.HLLW.Redist.C@mm runs, it displays a fake message, titled "Error Starting Program." The e-mail has various subject lines and attachments. This threat is written in the Microsoft Visual Basic programming language and is compressed with UPX.

W32.HLLW.Warpigs (Win32 Worm): This is a worm that contains backdoor Trojan functionality. It attempts to copy itself to computers that have weak administrator passwords. The existence of the file Discworld.exe is an indication of a possible infection. Connecting to a specific mIRC server and joining a specific channel to receive instructions performs the backdoor functionality. The default ports are 6666 and 6667.

W32.HLLW.Warpigs.B (Win32 Worm): This is a worm that contains backdoor Trojan functionality. It attempts to copy itself to computers that have weak administrator passwords. Connecting to a specific mIRC server and joining a specific channel to receive instructions performs the backdoor functionality. The default ports are 6666 and 6667.

W32/Israz-A (Alias: W32.Akosw@mm, WORM_ISRAZ.A, I-Worm.Israz, W32.Israz@mm, Win32.Israz.A, W32/Israz.worm) (Windows 95 Executable File Virus): This is an e-mail worm that spreads using its own SMTP engine. It also targets the KaZaA file sharing utility. Upon execution, the worm creates copies of itself in the Windows system folder with the filenames vShell.exe and Win32.exe. The worm also creates copies of itself in the Windows temp folder using the filenames Fun.exe, FAQ.exe, Q322593.exe, Support.exe, ToolBar.exe, and Wizard.exe. W32/Israz-A extracts a freeware SMTP Component ossmtp.dll and vUser.exe, the secondary worm component, into the Windows system folder. W32/Israz-A collects e-mail addresses from the Windows Address Book and sends itself as an attachment of an e-mail message with the various characteristics. It searches for the default KaZaA download folder. If the folder is found, the worm creates a copy of itself using one of the following filenames:

- XP Keys.exe
- OfficeXP Keys.exe
- NAV_2003 Crack.exe
- Doom_3 Crack.exe
- GTA Vice City Crack.exe

The worm also creates the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Win32 so that it contains the location of Win32.exe,
- HKLM\Software\Classes\txtfile\shell\open\command\ so that it contains the location of vShell.exe
- HKLM\Software\Symantec\ScriptBlocking so that it contains the string "Script Blocking."

W32.Jantic@mm (Win32 Worm): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all the contacts in the Outlook Address Book. W32.Jantic@mm is a Visual Basic application compiled to native code The e-mail has the following characteristics:

- Subject: You have a ecard!
- Attachment: attachment.exe (36, 864 bytes)

W32.Jantic.B@mm (Win32 Worm): This is a variant of W32.Jantic@mm. This variant is also a mass-mailing worm that uses Microsoft Outlook to send itself to all the contacts in the Outlook Address Book. The e-mail has the following characteristics:

- Subject: You have a ecard!
- Attachment: attachment.exe

or

- Subject: Technical Support - File you Requested.
- Attachment: attachment.exe

W32/Klexe-A (Aliases: WORM_KLEXE.A, I-Worm.Klexe, Win32.Klexe.A, W32.Klexe.Worm, W32/Klexe@MM) (Win32 Worm): This is a worm that uses Microsoft Outlook to send an e-mail to all addresses found in the address book. The e-mail arrives with a message. If the user clicks on the link, the ZIP file will be downloaded. Ecmsetup1.zip contains two files: a copy of W32/Klexe-A with the file name ecmsetup1.exe and a Trojan Troj/Klexe-A with the file name kl.exe. When executed, W32/Klexe-A (ecmsetup1.exe) will display a fake error message and will try to copy Troj/Klexe-A (kl.exe) to the following locations:

- C:\windows\startm~1\programs\startup\Windows Explorer.exe
- D:\windows\startm~1\programs\startup\Windows Explorer.exe
- E:\windows\startm~1\programs\startup\Windows Explorer.exe
- F:\windows\startm~1\programs\startup\Windows Explorer.exe

W32/Klexe-A will also use Troj/Klexe-A in attempt to send system information to a specific e-mail address.

W32.Mapson.C.Worm (Win32 Worm): This is a mass-mailing worm that sends itself to all the contacts in the MSN messenger contact list. The Subject line, Message body, and attachment vary. The attachment will have a .com, .exe, .scr, or .pif extension. Also, the e-mail may spoof the From field. The W32.Mapson.C.Worm attempts to spread itself through the KaZaA, KaZaA Lite, eDonkey2000, Gnucleus, LimeWire, Morpheus, and Grokster file-sharing networks, as well as through ICQ. It terminates some popular antivirus, firewall, and system-monitoring programs. It is written in the Borland Delphi programming language and is compressed with UPX.

W32.Moubot (Win32 Worm): This is a network-aware worm that copies itself as the following files:

- C$\WINNT\system32\fix.exe
- IPC$\WINNT\system32\fix.exe
- ADMIN$\WINNT\system32\fix.exe

W32.Moubot also has a backdoor functionality that allows its creator to control the compromised computer by using Internet Relay Chat (IRC). This threat is compressed with UPX.

W32/Mumu-C (Alias: Backdoor.MeteorShell.58) (Win32 Worm): This worm has been reported in the wild. It is a worm which spreads by copying itself to and executing itself on remote network shares with weak or no passwords. The worm drops the following files in the Windows system folder:

- LAST.EXE, detected as Troj/BGirlB-A
- KAVFIND.EXE, detected as Troj/Hacline-B
- IPCPASS.TXT, an innocuous file used by Troj/Hacline-B
- PSEXEC.EXE, a legitimate networking utility

It uses Troj/Hacline-B to identify potential victim IP addresses. The worm then copies itself to the remote computer and uses PSEXEC to execute itself remotely. W32/Mumu-C uses Troj/BGirlB-A to log keystrokes and steal passwords and then sends them to a preconfigured e-mail account at certain intervals.

W32/MyLife-M (Aliases: W32.Mylife.N@mm, W32/Mylife.m@MM, Win32.MyLife.M, WORM_MYLIFE.M, I-Worm.Mylife.m) (Win32 Worm): This worm has been reported in the wild. It is a worm that spreads via e-mail. Using Microsoft Outlook, W32/MyLife-M sends e-mails to addresses found in the Outlook address book and has various characteristics. The worm drops the file C:\MyLife.mpg and attempts to play it. If W32/MyLife-M is executed in the Windows system folder, the worm checks the time on the system clock. If the number of minutes past the hour is greater than or equal to 50, the worm attempts to delete all SYS files from the Windows folder, all files from the Windows system folder and all files and folders from drives D:, E:, and F: In order to run automatically when Windows starts up, the worm attempts to copy itself to the Windows system folder as a file named Shakira_1997_part_1_.Mpeg_.scr and creates the registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Win32

pointing to this file. The worm may also create a copy of itself named Julia_Roberts_Fucking_toilet.Mpeg_.scr in the Windows system folder.

W32.Sadon.867 (Win32 File Infector): This is a .exe file infector that spreads by appending an encrypted version of itself to the end of all the other .exe files, which are in the same folder as the virus. When a file that is infected with W32.Sadon.867 is executed, it decrypts the virus, runs it, and adds its encrypted infection routine to all the .exe files, which are in the same folder. Then, it passes control of the .exe file back to the infected host, so that you will not notice any difference in behavior.

W32.Sadon.dr (Win32 Dropper): This worm acts as a dropper for W32.Sadon.867, which affects all the .exe files in the current folder. Refer to the W32.Sadon.867 write-up above.

W32/Slanper-A (Aliases: W32/Slanper.worm, Win32/HLLW.Rejase.A, WORM_RANDEX.D, W32/Sluter, Win32.Slanper): This is an Internet worm that targets SMB/Windows shares using port 445. The worm may arrive with the filename msmsgri3.exe. Upon execution the worm installs itself as a background process with the same name and sets the registry entry:

- HKLM/Software/Microsoft/Windows/CurrentVersion/Run/mssyslanhelper

to contain the path to itself. It then generates a random list of IP numbers and attempts to connect to them using port 445 in attempt to copy itself to available shares. W32/Slanper-A also has some backdoor functionality. The worm also extracts a secondary component to the same folder with the filename payload.dat. If payload.dat is executed it sets the registry entry:

- HKLM/Software/Microsoft/Windows/CurrentVersion/Run/System Initialization

to contain the path to itself, initiates TCP port connection and runs in the background listening on open ports.

W32.Spex.Worm (Alias: P2P.Specx) (Win32 Worm): This is an encrypted worm that attempts to spread itself through the KaZaA and iMesh file-sharing networks. The worm drops itself to %System%\iexplore32.exe and to a variety of files in the %Windir%\Drivers32 folder. Then, it shares the %Windir%\Drivers32 folder through KaZaA and iMesh.

W32.Yaha.U@mm (Alias: I-Worm.Lentis.gen) (Win32 Worm): This worm is a variant of W32.Yaha.J@mm. It terminates some antivirus and firewall processes and uses its own SMTP engine to e-mail itself to all the contacts in the Windows Address Book, MSN Messenger, .NET Messenger, Yahoo Pager, and in all the files whose extensions contain the letters HT. The e-mail message has a randomly chosen subject line, message, and attachment name. The attachment will have a .com, .exe, or .scr file extension. It is written in the Microsoft C++ language and is compressed with ASPack.

W32.Yaha.Z@mm (Aliases: I-Worm.Lentin.c, W32/Yaha.d@mm, W32/Lentin.B@mm, Win32/Yaha.B@mm) (Win32 Worm): This is a variant of W32.Yaha.C@mm. It has been repacked to make it difficult for antivirus software to detect.

W32.Zokrim.V@mm (Win32 Worm): This is a variant of W32.Zokrim@mm. This variant is also a mass-mailing worm that uses Microsoft Outlook to send itself to all the contacts in the Outlook Address Book. The worm displays a message, titled "Valentina," when run. The e-mail has the following characteristics:

- Subject: "" and YOU
- Attachment: vale.exe

This threat is written in the Microsoft Visual Basic (VB) programming language.

W97M.Lexar.A (Word 97 Macro Virus): This is a macro virus that spreads between Microsoft Word documents. It bypasses the virus protection under Word 97 and has one payload that is activated on the 10th, 20th, and 30th of April, August, and December.

Win32.Melder (Win32 Virus): This is a harmless nonmemory resident parasitic Win32 virus. The virus itself is a Windows PE EXE file, written in Delphi. The virus size is about 46KB. The Melder virus infects .EXE files in the KaZaA file sharing network download directory. In case KaZaA is not installed, the virus fails to infect the computer. While infecting the virus writes itself to the beginning of the file. The virus contains the text string, "This Is A Infected File Infecting KaZaA Files..."

WM97/Adenu-A (Word 97 Macro Virus): WM97/Adenu-A lowers the Microsoft Office Security settings by setting the following registry entry:

- HKCU\Software\Microsoft\Office\9.0\Word\Security\Level=01

It also disables the following menu options within Microsoft Word:

- Tools|Macro
- Tools|Customize
- Tools|Templates and Add-Ins

WM97/Adenu-A creates the file GbcHS4664.VBS in the Windows system folder and sets the registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\GgcHS464 ="<Windows system folder>\GbcHS4664.VBS"

so that it is run when Windows is started. On 26th June WM97/Adenu-A replaces the contents of the active document with text in Filipino.

WM97/Revas-A (Word 97 Macro Virus): This is a macro virus that will make copies of infected files in the folder Office\Doc_Copy within the Microsoft Office folder.

WM97/ZWMVC-B (Word 97 Macro Virus): This is a simple macro virus that uses the name "zwmvc_macro" for the infected VBA module. The virus displays the message "Yet Again Porn Error" every time an infected document is opened or a clean document is infected.

Worm/Mofei.C (Alias: WORM_MOFEI.C) (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book. The worm arrives through e-mail in the following format:

- Subject: NEWS
- Attachment: lovegirls.exe

If executed, the worm copies itself in the \windows\%system% directory under the filename "lasvr32.exe." Additionally, the file "lasvr32.dll" (45.056KB) and "napw32.exe" (15.360KB) gets added in the \windows\%system% directory. So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run NavAgent32=C:\Windows\System\lasvr32.exe

Worm.Naliv (Network Worm): This is a network worm spreading over local and global networks. The worm itself is a Win32 application (PE EXE file) written in Borland C++. It has a file size of about 12K. When the worm is run it copies itself to the Windows system directory (the worm copy name can be various) and registers this file in the system registry auto-run key:

- HKLM\\SOFTWARE\Microsoft\Windows\CurrentVersion\Run NAV Live Update = %worm file name%

Worm/Ronoper.R (Alias: W32-Ronoper.R) (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Windows Address Book. The worm can also spread through the use of the file-sharing program KaZaA, as well as, the mIRC network. If executed, the worm copies itself in the \windows\ directory under the filenames "Melda.scr" and "Systools.exe." Additionally, the file "SysScript" gets added in the \windows\ directory to help in spreading over the mIRC network. The file "Melda.zip" as gets created. So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "System Toolkit"=C:\Windows\Systools.exe

It has the ability to disable various personal firewall applications and antivirus software programs.

WORM_SCORVAN.A (Aliases: W32.HLLW.Scorvan, Win32/HLLW.Scopiron.A, Worm.Win32.Scorvan) (Win32 Worm): This worm propagates via network shares and peer-to-peer file sharing networks. It displays several message boxes and stops, opens, and closes the CD drive. This worm runs on Windows 95, 98, ME, NT, 2000, and XP.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
AdwareDropper-A	A	CyberNotes-2003-04
Adware-SubSearch.dr	**dr**	**Current Issue**
AIM-Canbot	N/A	CyberNotes-2003-07
AprilNice	N/A	CyberNotes-2003-08
Backdoor.Acidoor	N/A	CyberNotes-2003-05
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Amitis.B	B	CyberNotes-2003-11
Backdoor.AntiLam.20.K	K	CyberNotes-2003-10
Backdoor.Apdoor	N/A	CyberNotes-2003-12
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Assasin.F	F	CyberNotes-2003-09
Backdoor.Badcodor	N/A	CyberNotes-2003-12
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Beasty.C	C	CyberNotes-2003-05
Backdoor.Beasty.Cli	Cli	CyberNotes-2003-10

Trojan	Version	CyberNotes Issue #
Backdoor.Beasty.D	D	CyberNotes-2003-06
Backdoor.Beasty.E	E	CyberNotes-2003-06
Backdoor.Bigfoot	N/A	CyberNotes-2003-09
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.Bridco	N/A	CyberNotes-2003-06
Backdoor.CamKing	N/A	CyberNotes-2003-10
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Cmjspy	N/A	CyberNotes-2003-10
Backdoor.Cmjspy.B	**B**	**Current Issue**
Backdoor.CNK.A	A	CyberNotes-2003-10
Backdoor.CNK.A.Cli	Cli	CyberNotes-2003-10
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	N/A	CyberNotes-2003-05
Backdoor.Death.Cli	Cli	CyberNotes-2003-10
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Delf.Cli	Cli	CyberNotes-2003-10
Backdoor.Delf.F	F	CyberNotes-2003-07
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.Dsklite	**N/A**	**Current Issue**
Backdoor.Dsklite.cli	**cli**	**Current Issue**
Backdoor.Dvldr	N/A	CyberNotes-2003-06
Backdoor.EggDrop	N/A	CyberNotes-2003-08
Backdoor.Fatroj	N/A	CyberNotes-2003-10
Backdoor.Fatroj.Cli	Cli	CyberNotes-2003-10
Backdoor.Fluxay	N/A	CyberNotes-2003-07
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.FTP_Ana.C	C	CyberNotes-2003-07
Backdoor.FTP_Ana.D	D	CyberNotes-2003-08
Backdoor.Fxdoor	N/A	CyberNotes-2003-10
Backdoor.Fxdoor.Cli	Cli	CyberNotes-2003-10
Backdoor.Graybird	N/A	CyberNotes-2003-07
Backdoor.Graybird.B	B	CyberNotes-2003-08
Backdoor.Graybird.C	C	CyberNotes-2003-08
Backdoor.Graybird.D	**D**	**Current Issue**
Backdoor.Grobodor	N/A	CyberNotes-2003-12
Backdoor.Guzu.B	**B**	**Current Issue**
Backdoor.HackDefender	N/A	CyberNotes-2003-06
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Aladinz.C	**C**	**Current Issue**
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Comiz	N/A	CyberNotes-2003-11
Backdoor.IRC.Lampsy	N/A	CyberNotes-2003-10

Trojan	Version	CyberNotes Issue #
Backdoor.IRC.Ratsou	N/A	CyberNotes-2003-10
Backdoor.IRC.Ratsou.B	B	CyberNotes-2003-11
Backdoor.IRC.Ratsou.C	C	CyberNotes-2003-11
Backdoor.IRC.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.Kaitex.D	D	CyberNotes-2003-09
Backdoor.Kalasbot	N/A	CyberNotes-2003-09
Backdoor.Khaos	N/A	CyberNotes-2003-04
Backdoor.Kilo	N/A	CyberNotes-2003-04
Backdoor.Kodalo	**N/A**	**Current Issue**
Backdoor.Kol	N/A	CyberNotes-2003-06
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.Lanfilt.B	**B**	**Current Issue**
Backdoor.LeGuardien.B	B	CyberNotes-2003-10
Backdoor.Litmus.203.c	c	CyberNotes-2003-09
Backdoor.LittleWitch.C	C	CyberNotes-2003-06
Backdoor.Longnu	N/A	CyberNotes-2003-06
Backdoor.Marotob	N/A	CyberNotes-2003-06
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.MindControl	**N/A**	**Current Issue**
Backdoor.Monator	N/A	CyberNotes-2003-08
Backdoor.Mots	N/A	CyberNotes-2003-11
Backdoor.MSNCorrupt	N/A	CyberNotes-2003-06
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Nickser	**N?A**	**Current Issue**
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Optix.04.d	04.d	CyberNotes-2003-04
Backdoor.OptixDDoS	N/A	CyberNotes-2003-07
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.OptixPro.12.b	12.b	CyberNotes-2003-07
Backdoor.OptixPro.13	13	CyberNotes-2003-09
Backdoor.Peers	N/A	CyberNotes-2003-10
Backdoor.Plux	N/A	CyberNotes-2003-05
Backdoor.Pointex	N/A	CyberNotes-2003-09
Backdoor.Pointex.B	B	CyberNotes-2003-09
Backdoor.Private	N/A	CyberNotes-2003-11
Backdoor.Prorat	N/A	CyberNotes-2003-13
Backdoor.PSpider.310	310	CyberNotes-2003-05
Backdoor.Queen	N/A	CyberNotes-2003-06
Backdoor.Ratega	N/A	CyberNotes-2003-09
Backdoor.Recerv	N/A	CyberNotes-2003-09
Backdoor.Redkod	N/A	CyberNotes-2003-05
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01

Trojan	Version	CyberNotes Issue #
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.Rsbot	N/A	CyberNotes-2003-07
Backdoor.SchoolBus.B	B	CyberNotes-2003-04
Backdoor.Sdbot.C	C	CyberNotes-2003-02
Backdoor.Sdbot.D	D	CyberNotes-2003-03
Backdoor.Sdbot.E	E	CyberNotes-2003-06
Backdoor.Sdbot.F	F	CyberNotes-2003-07
Backdoor.Sdbot.G	G	CyberNotes-2003-08
Backdoor.Sdbot.H	H	CyberNotes-2003-09
Backdoor.Sdbot.L	L	CyberNotes-2003-11
Backdoor.Sdbot.M	M	CyberNotes-2003-13
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Simali	N/A	CyberNotes-2003-09
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Slao	N/A	CyberNotes-2003-11
Backdoor.Snami	N/A	CyberNotes-2003-10
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.Socksbot	N/A	CyberNotes-2003-06
Backdoor.Softshell	N/A	CyberNotes-2003-10
Backdoor.Stealer	**N/A**	**Current Issue**
Backdoor.SubSari.15	15	CyberNotes-2003-05
Backdoor.SubSeven.2.15	2.15	CyberNotes-2003-05
Backdoor.Syskbot	N/A	CyberNotes-2003-08
Backdoor.SysXXX	N/A	CyberNotes-2003-06
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Tankedoor	N/A	CyberNotes-2003-07
Backdoor.Trynoma	N/A	CyberNotes-2003-08
Backdoor.Turkojan	N/A	CyberNotes-2003-07
Backdoor.Udps.10	1	CyberNotes-2003-03
Backdoor.UKS	N/A	CyberNotes-2003-11
Backdoor.Unifida	N/A	CyberNotes-2003-05
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Winet	N/A	CyberNotes-2003-11
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.XTS	N/A	CyberNotes-2003-08
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdemon.126	126	CyberNotes-2003-10
Backdoor.Zdown	N/A	CyberNotes-2003-05
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zombam	N/A	CyberNotes-2003-08
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	N/A	CyberNotes-2003-05
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	N/A	CyberNotes-2003-05

Trojan	Version	CyberNotes Issue #
BackDoor-AQT	N/A	CyberNotes-2003-05
BackDoor-ARR	ARR	CyberNotes-2003-06
Backdoor-ARU	ARU	CyberNotes-2003-06
BackDoor-ARX	ARX	CyberNotes-2003-06
BackDoor-ARY	ARY	CyberNotes-2003-06
BackDoor-ASD	ASD	CyberNotes-2003-07
BackDoor-ASL	ASL	CyberNotes-2003-07
BackDoor-ASW	ASW	CyberNotes-2003-08
BackDoor-ATG	ATG	CyberNotes-2003-09
BackDoor-AUP	N/A	CyberNotes-2003-11
BackDoor-AVF	AVF	CyberNotes-2003-12
BackDoor-AVH	AVH	CyberNotes-2003-12
BackDoor-AVO	AVO	CyberNotes-2003-12
BackDoor-AXC	**AXC**	**Current Issue**
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/CheckESP	N/A	CyberNotes-2003-12
BDS/Ciadoor.10	10	CyberNotes-2003-07
BDS/Evilbot.A	A	CyberNotes-2003-09
BDS/Evolut	N/A	CyberNotes-2003-03
BDS/PowerSpider.A	A	CyberNotes-2003-11
Daysun	N/A	CyberNotes-2003-06
DDoS-Stinkbot	N/A	CyberNotes-2003-08
DoS-iFrameNet	N/A	CyberNotes-2003-04
Download.Trojan.B	B	CyberNotes-2003-13
Downloader.BO.B	B	CyberNotes-2003-10
Downloader.BO.B.dr	B.dr	CyberNotes-2003-10
Downloader-BN.b	BN.b	CyberNotes-2003-13
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Downloader-BW	N/A	CyberNotes-2003-05
Downloader-BW.b	BW.b	CyberNotes-2003-06
Downloader-BW.c	BW.c	CyberNotes-2003-07
ELF_TYPOT.A	A	CyberNotes-2003-13
ELF_TYPOT.B	B	CyberNotes-2003-13
Exploit-IISInjector	N/A	CyberNotes-2003-03
Gpix	N/A	CyberNotes-2003-08
Hacktool.PWS.QQPass	N/A	CyberNotes-2003-06
ICQPager-J	N/A	CyberNotes-2003-05
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.ap	N/A	CyberNotes-2003-05
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC/Flood.br	br	CyberNotes-2003-06
IRC/Flood.bu	bu	CyberNotes-2003-08
IRC/Flood.cd	cd	CyberNotes-2003-11
IRC/Flood.cm	cm	CyberNotes-2003-13

Trojan	Version	CyberNotes Issue #
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
IRC-Vup	N/A	CyberNotes-2003-09
JS.Fortnight.B	B	CyberNotes-2003-06
JS.Seeker.J	J	CyberNotes-2003-01
JS/Fortnight.c@M	c	CyberNotes-2003-11
JS/Seeker-C	C	CyberNotes-2003-04
JS/StartPage.dr	dr	CyberNotes-2003-11
JS_WEBLOG.A	A	CyberNotes-2003-05
Keylogger.Cone.Trojan	**N/A**	**Current Issue**
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Kjie	N/A	CyberNotes-2003-12
Keylog-Perfect.dr	dr	CyberNotes-2003-09
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Keylog-Yeehah	N/A	CyberNotes-2003-12
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
MultiDropper-FD	N/A	CyberNotes-2003-01
Pac	N/A	CyberNotes-2003-04
ProcKill-AE	N/A	CyberNotes-2003-05
ProcKill-AF	N/A	CyberNotes-2003-05
ProcKill-AH	AH	CyberNotes-2003-08
ProcKill-AJ	AJ	CyberNotes-2003-13
ProcKill-Z	N/A	CyberNotes-2003-03
Proxy-Guzu	N/A	CyberNotes-2003-08
Proxy-Migmaf	**N/A**	**Current Issue**
PWS-Aileen	N/A	CyberNotes-2003-04
PWSteal.ABCHlp	N/A	CyberNotes-2003-12
PWSteal.AlLight	N/A	CyberNotes-2003-01
PWSteal.Hukle	N/A	CyberNotes-2003-08
PWSteal.Kipper	N/A	CyberNotes-2003-10
PWSteal.Lemir.105	105	CyberNotes-2003-10
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Rimd.B	B	CyberNotes-2003-10
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWSteal.Snatch	N/A	CyberNotes-2003-10
PWSteal.Sysrater	N/A	CyberNotes-2003-12
PWS-Tenbot	N/A	CyberNotes-2003-01
PWS-Truebf	N/A	CyberNotes-2003-13
PWS-Watsn	N/A	CyberNotes-2003-10
PWS-Wexd	**N/A**	**Current Issue**
PWS-WMPatch	N/A	CyberNotes-2003-07
PWS-Yipper	N/A	CyberNotes-2003-10
QDel359	359	CyberNotes-2003-01
QDel373	373	CyberNotes-2003-06
Qdel374	374	CyberNotes-2003-06
Qdel375	375	CyberNotes-2003-06
Qdel376	376	CyberNotes-2003-07
QDel378	378	CyberNotes-2003-08

Trojan	Version	CyberNotes Issue #
QDel379	369	CyberNotes-2003-09
QDel390	390	CyberNotes-2003-13
QDel391	391	CyberNotes-2003-13
QDel392	392	CyberNotes-2003-13
QDial11	**1**	**Current Issue**
QDial6	6	CyberNotes-2003-11
Renamer.c	N/A	CyberNotes-2003-03
Reom.Trojan	N/A	CyberNotes-2003-08
StartPage-G	G	CyberNotes-2003-06
Startpage-N	N	CyberNotes-2003-13
Stoplete	N/A	CyberNotes-2003-06
Swizzor	N/A	CyberNotes-2003-07
Tellafriend.Trojan	N/A	CyberNotes-2003-04
Tr/Decept.21	21	CyberNotes-2003-07
Tr/DelWinbootdir	N/A	CyberNotes-2003-07
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
Tr/SpBit.A	A	CyberNotes-2003-04
Tr/VB.t	T	CyberNotes-2003-11
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Dloader-BO	BO	CyberNotes-2003-02
Troj/Hacline-B	B	CyberNotes-2003-13
Troj/IRCBot-C	C	CyberNotes-2003-11
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Mystri-A	A	CyberNotes-2003-13
Troj/PcGhost-A	A	CyberNotes-2003-13
Troj/Peido-B	B	CyberNotes-2003-10
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Sandesa-A	**A**	**Current Issue**
Troj/Slacker-A	A	CyberNotes-2003-05
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/TKBot-A	A	CyberNotes-2003-04
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_RACKUM.A	A	CyberNotes-2003-05
Trojan.AprilFool	N/A	CyberNotes-2003-08
Trojan.Barjac	N/A	CyberNotes-2003-05
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Downloader.Aphe	N/A	CyberNotes-2003-06
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Grepage	N/A	CyberNotes-2003-05
Trojan.Guapeton	N/A	CyberNotes-2003-08
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.Kaht	N/A	CyberNotes-2003-10
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Lear	N/A	CyberNotes-2003-10

Trojan	Version	CyberNotes Issue #
Trojan.Mumuboy	N/A	CyberNotes-2003-13
Trojan.Myet	N/A	CyberNotes-2003-12
Trojan.Poetas	**N/A**	**Current Issue**
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	N/A	CyberNotes-2003-05
Trojan.PopSpy	N/A	CyberNotes-2003-11
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	N/A	CyberNotes-2003-06
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Sarka	**N/A**	**Current Issue**
Trojan.Sidea	N/A	CyberNotes-2003-12
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Trojan.Windelete	**N/A**	**Current Issue**
Uploader-D	D	CyberNotes-2003-06
Uploader-D.b	D.b	CyberNotes-2003-07
VBS.ExitWin	N/A	CyberNotes-2003-12
VBS.Kasnar	N/A	CyberNotes-2003-06
VBS.Moon.B	B	CyberNotes-2003-02
VBS.StartPage	N/A	CyberNotes-2003-02
VBS.Trojan.Lovcx	N/A	CyberNotes-2003-05
VBS.Zizarn	N/A	CyberNotes-2003-09
VBS/Fourcourse	N/A	CyberNotes-2003-06
W32.Adclicker.C.Trojan	C	CyberNotes-2003-09
W32.Bambo	**N/A**	**Current Issue**
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.CVIH.Trojan	N/A	CyberNotes-2003-06
W32.Laorenshen.Trojan	**N/A**	**Current Issue**
W32.Noops.Trojan	N/A	CyberNotes-2003-09
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Systentry.Trojan	N/A	CyberNotes-2003-03
W32.Trabajo	**N/A**	**Current Issue**
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32/Igloo-15	N/A	CyberNotes-2003-04
Xin	N/A	CyberNotes-2003-03

Adware-SubSearch.dr (Alias: Startpage-M): This Trojan silently installs the Adware-SubSearch application. This dropper Trojan has been circulating with the filenames sub2_1C.exe and sub2b.exe and creates the file SbSrch_V2.dll and SbSrch_V2.dll in the WINDOWS SYSTEM (%SysDir%) directory.

BackDoor-AXC: This is a remote access Trojan written in Microsoft Visual Basic. When run on the victim machine, a fake error message is displayed. Port 88 is opened or listening for remote commands The Trojan attempts to access a remote server (on port 777) The malicious user connects to the victim machine on port 88 via HTTP, and can execute remote commands such as:

- open CD tray
- close CD tray
- send welcome message to victim

Backdoor.Cmjspy.B: This is a Backdoor Trojan Horse that logs keystrokes. Backdoor.Cmjspy.B is a slight variant of Backdoor.Cmjspy. The functionality is the basically the same; however, the names of the files and registry keys that this Trojan creates differ. It is written in the Borland Delphi programming language and is UPX-packed.

Backdoor.Dsklite (Alias: Backdoor.DskLite.b): This is a Backdoor Trojan Horse that gives the author of the Trojan full access to an infected computer. By default, this Trojan listens on port 890. When Backdoor.Dsklite is executed for the first time, it displays a fake message, with the title "Error." It is written in Microsoft Visual Basic (VB). The VB run-time libraries are required to execute Backdoor.Dsklite.

Backdoor.Dsklite.cli: This is the client side of Backdoor.Dsklite, and allows unauthorized access to an infected computer. This Trojan Horse is written in Microsoft Visual Basic and may or may not be packed. Backdoor.Dsklite.cli uses configurable ports to connect a client to a server. A client may create multiple server profiles. When run, this Trojan gives the malicious user the ability to:

- Stop antivirus and firewall software on the server.
- Manipulate files and directories.
- Edit registries.
- Capture screen shots and password information.
- Enable the Webcam.
- Stop the server processes altogether.
- Chat with and harass the user of the server.

It stores its information in HKEY_LOCAL_MACHINE\Software\DSK. Further, the malicious user may save the server executable in a UPX- or FSG-packed file, or in an unpacked file.

Backdoor.Guzu.B (Aliases: BackDoor-AWI, Trojanproxy.Win32.Guzuloh): The Backdoor.Guzu.B Trojan Horse allows its creator to send e-mail using your computer. When it is run, it adds the string value, "Services"="<the file name of the hacktool>." to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the hacktool file runs when you start Windows. It registers its process as a service if the hacktool is running on a Windows 95/98/ME computer. It opens a randomly chosen TCP port to listen for the Trojan's creator, allowing him/her to send numerous e-mail messages through a compromised computer. It uses its own SMTP engine and mx1.hotmail.com as an e-mail server to send the following e-mail:

- From: fakeaddres@hotmail.com
- To: stuff4m3@hotmail.com
- Subject: The subject line contains the TCP port number used by the hacktool and the compromised computer's IP address.
- Message: Proxy is running..

Backdoor.IRC.Aladinz.C (Aliases: Worm.Win32.Ircobus, Worm.Win32.Randon.p): This is an IRC Trojan Horse that gives its creator full control over a compromised system. The Trojan may be downloaded by the Trojan.Downloader.Aphe from the Web site, www.ircx-vanguard.com. The existence of the file uqir.exe is an indication of a possible infection.

Backdoor.Graybird.D: This is a variant of Backdoor.Graybird. This Trojan Horse gives its creator unauthorized access to your computer. The existence of the file, Svch0st.exe, is an indication of a possible infection. This threat is written in Borland Delphi and compressed with ASPack.

Backdoor.Kodalo: This is a Backdoor Trojan Horse that gives the author of the Trojan full access to an infected computer. By default, the Trojan listens on port 25025, 25026, or 25044. When Backdoor.Kodalo is executed, it copies itself as %System%\PowerManager.exe. The file attributes are set to Archive and

Hidden. The Trojan adds the value, "Power Manager"="%System%\powermanager.exe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

and registers itself as a service process.

Backdoor.Lanfilt.B: This is a variant of Backdoor.Lanfilt. It allows its creator unauthorized access to a compromised computer and attempts to disable some antivirus, firewall, and system-monitoring programs by terminating processes. It is a Delphi application that may be compressed with UPX. The Trojan displays a message. Refer to Step 4 of the "Technical Details" section for an illustration.

Backdoor.MindControl: (Alias: Backdoor.MindControl.50): The Backdoor.MindControl Backdoor Trojan Horse gives its creator full control over your computer. It opens port 23, by default. It is written in the Visual Basic (VB) programming language and needs the VB run-time libraries installed for it to work. When Backdoor.MindControl is executed, it copies itself as %Windir%\Hellraider.exe and adds the value, "Fhzepayi"="%Windows%\Hellraider.exe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

and adds the value, "Badx"="%Windows%\Hellraider.exe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

Backdoor.Nickser: This is a backdoor Trojan program. The Trojan itself is a Windows PE EXE file about 136KB in length (when compressed by TeLock, the decompressed size is about 270KB). It is written in Microsoft Visual C++. When run the backdoor copies itself under the name lsass.exe name to the Windows directory and registers itself in the system registry auto-run key:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run UserInitialization = %WinDir%\lsass.exe

Nickser then reads its "master's" instructions from an encrypted script file located on the Web at http://go.xmain.da.ru.

Backdoor.Stealer: This is a backdoor Trojan Horse. It gives its creator full control over your computer and opens ports 60101 and 16999. The Trojan is written in the Delphi programming language. When Backdoor.Stealer is executed, it copies itself as %Windir%\Windll.exe and adds the value, "Windll.exe"="%Windows%\Windll.exe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

The Trojan also adds the values:

- "1"="<Your IP Address>"
- "2"="<Your IP Address>"
- "3"="<Your IP Address>"
- "LastIP"="<Your IP Address>"

to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Obsidian Industries\MSN 6 Log Thief.

Keylogger.Cone.Trojan (Aliases: Keylog-Perfect.dr, KeyLogger.Win32.PerfectKeyLogger.141): This is a keylogger that tracks various user activities. It periodically sends its tracking logs to a remote malicious user using e-mail or ftp.

Proxy-Migmaf: This Trojan acts as a reverse proxy on the victim machine, redirecting HTTP requests to a remote web server. Multiple versions of this threat are known to exist and have been packed with tElock. By routing HTTP requests through the reverse proxy running on victim machines, the malicious user is able to mask the genuine source IP of the web server hosting the web content (typically pornographic). Upon execution, the Trojan creates a mutex of name:

- REQUEST_MANAGE_SUBSYSTEM

The Trojan checks the keyboard layout of the victim machine in order to stop it functioning on Russian machines (those with Russian keyboard configuration at least). Values with the following key are used to determine the layout(s):

- HKEY_CURRENT_USER\Keyboard Layout\Preload

The Trojan does not copy itself on the victim machine, but merely adds the following Registry hook pointing to the file that was executed:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Login Service" = (points to the file executed)

After a short sleep, the Trojan attempts to access the following site:

- www.microsoft.com

Subsequently, (garbage) data is sent to this site (port 80) as a means of testing available bandwidth. A disclaimer in the body of the Trojan highlights this. In order to help prevent identification of the server that genuinely hosts the web content, the Trojan does not connect directly to the relevant IP. Instead, it cycles through various A.B.C.D combinations, constructed by varying each octet between certain values.

PWS-Wexd (Alias: Trojan.Spy.Wexd): This is a password stealing Trojan. When executed, the below window is displayed: There are three components to this Trojan:

- ebina.exe
- thost.dll
- osyst32.dll

The Trojan drops the following files into the %WINDIR% directory when run:

- dod__10d001.ux (encrypted)
- ech.exe (Trojan body)
- mct.sys (log file)
- sct.sys (log file)
- win.txt (encrypted information)
- wini.sys (contains information about system's IP address)

Where %WINDIR% is C:\windows or C:\winnt When various websites are visited, the Trojan will record the keyboard and mouse inputs entered and save the information in encrypted format. The file is sent via the SMTP server smtp.bol.com.br to the author's e-mail.

QDial11: This Trojan tries to use an installed Modem to call an expensive 0190 872xxx number. After execution, the Trojan starts dialing without displaying any dialog or warning messages and deletes itself from the harddrive. The Trojan tries to terminate application with the following filenames:

- 0190Alarm.exe
- 0190Killer.exe
- Warn0910.exe
- SmartSurfer.exe
- hh.exe
- dc.exe

It does not make any changes to the registry or system files.

Troj/Sandesa-A (Aliases: TrojanDownloader.Win32.Sandesa.11, DoS.Win32.Nenet, Flooder.UDP.Pjam.35, Trojan.BAT.Passer.a): This is a Trojan downloader program that drops the file C:\system.dll and attempts to download a selection of malware and malicious user tools to the user's system.

Trojan.Poetas: This Trojan causes system instability and can cause your computer to crash. It copies itself to the predetermined folders on all the local drives and is not network aware. After Trojan.Poetas copies itself, it launches the file that it copied. Eventually this process depletes the system resources, causing the system to crash. Is written in the Delphi programming language.

Trojan.Sarka: This is a Trojan Horse that consumes all CPU resources. The Trojan overwrites legitimate Windows executables like command.com and notepad.exe with a copy of itself. You may need to press the computer's reset button to reboot the computer.

Trojan.Windelete: This Trojan is written in Microsoft Visual Basic. When Trojan.Windelete is run, it deletes the C:\Windows folder. This is hard coded in the Trojan does not depend on the variable of the Windows installation folder (%Windir%). This Trojan does not set the registry keys and does not drop files.

W32.Bambo: This is a Trojan Horse that attempts to steal WebMoney Keeper files, capture clipboard data, and log key strokes.

W32.Laorenshen.Trojan: This is a Trojan Horse that tries to delete files and block the use of the computer's normal programs. It is compressed with UPX and ASPack.

W32.Trabajo: This is a Trojan Horse that uses a standard Windows folder icon to deceive you into believing that it is a real folder. If you double-click the Trojan's folder icon, the Trojan will be executed. When W32.Trabajo runs, it copies itself as the following:

- %Windir%\Msgsrv32.com
- %System%\Rundll32.com
- %System%\Wininit.com

The Trojan adds the value, "Wininit"="%System%\wininit.com," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

and adds the value, "Rundll32"="%System%\rundll32.com," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

It also adds the value. "Msgsrv32"="%Windir%\msgsrv32.com," to the registry key:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run